KEAMANAN INFORMASI

Penulis

Angga Aditya Permana
Nur Hayati
Abdurrasyid
Rima Rizqi Wijayanti
Marniyati H. Botutihe
Irmawati
Iwan Adhicandra
Yendi Putra
Arief Yanto Rukmana
Suwito Pomalingo
Shah Khadafi
Agung Susilo Yuda Irawan
Jarwo

Get Press Indonesia

ISBN 978-623-198-569-9

KEAMANAN INFORMASI

Angga Aditya Permana
Nur Hayati
Abdurrasyid
Rima Rizqi Wijayanti
Marniyati H. Botutihe
Irmawati
Iwan Adhicandra
Yendi Putra
Arief Yanto Rukmana
Suwito Pomalingo
Shah Khadafi
Agung Susilo Yuda Irawan
Jarwo

GET PRESS INDONESIA

KEAMANAN INFORMASI

Penulis :
Angga Aditya Permana
Nur Hayati
Abdurrasyid
Rima Rizqi Wijayanti
Marniyati H. Botutihe
Irmawati
Iwan Adhicandra
Yendi Putra
Arief Yanto Rukmana
Suwito Pomalingo
Shah Khadafi
Agung Susilo Yuda Irawan
Jarwo

ISBN : 978-623-198-569-9

Editor : Diana Purnama Sari, S.E., M.E
Penyunting : Ari Yanto, M.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, 8 Agustus 2023

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Keamanan Informasi ini.

Buku Ini Membahas Sejarah dan introduction Keamanan Informasi, Perkenalan Kriptografi, Symetric Encryption, Asymetric Encryption, Steganalisis, Watermarking, Wrireless security, Web Security, IP (*Internet Protocol*) Security, Firewall, Intrusion Detection System, Adhoc Networking, Mobile Adhoc Networking.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, Juli 2023

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **ii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xii**
BAB 1 SEJARAH DAN INTRODUCTION KEAMANAN INFORMASI **1**
1.1 Pendahuluan 1
1.2 Sejarah Keamanan Informasi 7
1.3 Keamanan Internet of Things (IoT) 9
1.4 Keamanan Blockchain 12
1.5 Keamanan Quantum 14
1.6 Orang yang Terlibat dalam Keamanan Informasi 16
1.7 Badan Keamanan Negara di Dunia 19
1.8 Badan Keamanan Negara di Indonesia 22
DAFTAR PUSTAKA 27
BAB 2 PERKENALAN KRIPTOGRAFI **29**
2.1 Sejarah Kriptografi 29
2.2 Algoritma Kriptografi 32
2.2.1 Kriptogradi Klasik 34
2.2.2 Kriptografi Modern 40
DAFTAR PUSTAKA 41
BAB 3 SYMMETERIC ENCRYPTION **43**
3.1 Pendahuluan 43
3.2 Pertukaran Kunci 48
3.3 Advanced Encryption Standard (AES) 49
3.4 Kelebihan dan kekurangan enkripsi simetris 53
DAFTAR PUSTAKA 56
BAB 4 ASYMMETRIC ENCRYPTION **57**
4.1 Pendahuluan 57
4.2 Asymmetric Encription 59
4.3 Enkripsi kunci publik 60

4.4 Contoh penggunaan asymmetric encryption 61
4.5 Infratruktur kunci publik 62
4.6 Keuntungan dan Kelemahan penggunaan asymmetric encryption 63
4.7 Membuat enkripsi asimetrik sendiri 64
DAFTAR PUSTAKA 67
BAB 5 STEGANALISIS 69
5.1 Pendahuluan 69
5.2 Metode Steganalisis 71
5.2.1 Analisis Statistik 71
5.2.2 Analisis Domain Spasial 72
5.2.3 Analisis Domain Frekuensi 72
5.2.4 Analisis Redundansi 72
5.2.5 Analisis Keseragaman 72
5.2.6 Analisis Entropi 72
5.2.7 Analisis Teknik Steganografi Yang Diketahui 73
5.3 Algoritma Steganalisis 73
5.4 Steganalisis Audio 73
5.5 Steganalisis Gambar 74
5.6 Steganalisis Video 74
5.7 Steganalisis Tanda Tangan 75
5.8 Steganalisis Statistik 75
5.9 Steganalisis Mendalam 75
5.10 Jenis-jenis Steganalisis 76
5.10.1 Histogram Analysis 76
5.10.2 RS Analysis 76
5.10.3 Correlation Analysis 76
5.10.4 Noise Analysis 77
5.10.5 Visual Artifact Analysis 77
10.5.6 Compression Analysis 77
DAFTAR PUSTAKA 78
BAB 6 WATERMARKING 81
6.1 Pendahuluan 81

6.1.1 Pengantar Watermarking Digital 83
6.1.2 Watermarking Dalam Keamanan Informasi 88
6.2 Dasar-Dasar Watermarking Digital 89
6.3 Teknik Penanaman Watermark 91
6.3.1 Watermarking di Domain Spasial 91
6.3.2 Watermarking di Domain Frekuensi 92
6.3.3 Watermarking di Domain Transformasi 94
6.3.4 Watermarking di Domain Spectrum 95
6.3.5 Watermarking Berbasis Kuantisasi 96
6.4 Teknik Ekstraksi dan Deteksi Watermark 97
6.4.1 Metode Ekstraksi Watermark 98
6.4.2 Deteksi dan Pemulihan Watermark 99
6.5 Ketahanan dan Keamanan Watermarking 100
6.5.1 Keamanan Watermark terhadap Serangan Jahat 100
6.6 Aplikasi Watermarking 102
DAFTAR PUSTAKA 105
BAB 7 WIRELESS SECURITY 107
7.1 Pendahuluan 107
7.1.1 Definisi Wireless Security 107
7.1.2 Sejarah dan Perkembangan Wireless Security 107
7.1.3 Pentingnya Wireless Security 108
7.2 Dasar-Dasar Wireless Security 108
7.2.1 Cara Kerja Wireless Networks 108
7.2.2 Risiko dan Ancaman Keamanan dalam Wireless Networks 109
7.2.3 Prinsip-prinsip Keamanan Wireless 109
7.3 Protokol Keamanan Wireless 110
7.3.1 Wired Equivalent Privacy (WEP) 110
7.3.2 Wi-Fi Protected Access (WPA) 110
7.3.3 Wi-Fi Protected Access II (WPA2) 110
7.3.4 Wi-Fi Protected Access III (WPA3) 111
7.3.5 Lainnya (TKIP, AES, etc.) 111
7.4 Alat dan Teknik Keamanan Wireless 111

7.4.1 Firewall dan Intrusion Prevention Systems 111
7.4.2 Virtual Private Networks (VPNs) 112
7.4.3 Network Access Control (NAC) 112
7.4.4 Wireless Intrusion Prevention Systems (WIPS) 112
7.5 Praktik Terbaik Keamanan Wireless 113
7.5.1 Mendefinisikan Kebijakan Keamanan Wireless 113
7.5.2 Menggunakan Enkripsi Kuat 113
7.5.3 Mengubah Default SSID dan Password 113
7.5.4 Menyembunyikan SSID 113
7.5.5 Mengaktifkan MAC Address Filtering 113
7.6 Ancaman dan Serangan Keamanan Wireless Terkini 114
7.6.1 Eavesdropping dan Interception 114
7.6.2 Man-In-The-Middle Attacks 114
7.6.3 Denial of Service (DoS) Attacks 114
7.6.4 Network Injection Attacks 115
7.7 Masa Depan Keamanan Wireless 115
7.7.1 Perkembangan Teknologi Terbaru 115
7.7.2 Tantangan dan Peluang 115
7.8 Studi Kasus 116
7.8.1 Kasus Pelanggaran Keamanan Wireless 116
7.8.2 Solusi dan Pelajaran yang Dapat Dipetik 116
7.9 Kesimpulan 117
DAFTAR PUSTAKA 119
BAB 8 WEB SECURITY 121
8.1 Pendahuluan 121
8.1.1 Perkembangan Website: 123
8.1.2 Teknologi yang digunakan dalam membangun sebuah website: 123
8.2 Jenis-jenis website 125
8.3 Bahasa pemrograman yang digunakan membuat website: 126
8.4 Domain dan Hosting 127
8.4.1 Domain 127

8.4.2 Hosting....129
8.5 Pendekatan atau Metodologi dalam Melakukan Pentrationtest Website....132
8.6 Jenis-Jenis Serangan Pada Website....134
8.6.1 Serangan SQL Injection....134
8.6.2 Serangan Cross-Site Scripting (XSS)....137
8.6.3 Serangan Cross-Site Request Forgery (CSRF)....140
8.6.4 Serangan DDoS (Distributed Denial of Service)....144
8.6.5 Serangan Brute Force....147
8.6.6 Serangan Man-in-the-Middle (MitM)....151
8.6.7 Serangan Pharming....154
8.6.8 Serangan File Inclusion....157
8.6.9 Serangan Server Side Request Forgery (SSRF)....161
8.6.10 Serangan Clickjacking....164
8.7 Langkah-langkah pencegahan serangan pada website....167
8.7.1 Serangan SQL Injection....167
8.7.2 Serangan Cross-Site Scripting (XSS)....169
8.7.3 Serangan Cross-Site Request Forgery (CSRF)....170
8.7.4 Serangan DDoS (Distributed Denial of Service)....172
8.7.5 Serangan Brute Force....174
8.7.6 Serangan Man-in-the-Middle (MitM)....176
8.7.7 Serangan Pharming....177
8.7.8 Serangan File Inclusion....178
8.7.9 Serangan Server Side Request Forgery (SSRF)....180
8.7.10 Serangan Clickjacking....182
DAFTAR PUSTAKA....183
BAB 9 IP (INTERNET PROTOCOL) SECURITY.... 187
9.1 Pendahuluan....187
9.2 Dasar-Dasar IP....189
9.2.1 Struktur Paket IP....190
9.3 Ancaman dan Serangan Keamanan IP....192
9.4 Protokol Keamanan IP....194
9.5 Mekanisme Keamanan IP....196

9.6 Praktik Terbaik Keamanan IP 198
9.7 Keamanan IP di Jaringan Nirkabel 200
9.8 Keamanan IP di Internet of Things (IoT) 203
9.9 Kesimpulan 205
DAFTAR PUSTAKA 208
BAB 10 FIREWALL 213
10.1 Pendahuluan 213
10.1.1 Definisi dan fungsi Firewall 214
10.1.2 Sejarah dan evolusi Firewall 215
10.1.3 Jenis-jenis Firewall 216
10.1.4 Arsitektur Firewall 218
10.2 Cara Kerja Firewall 220
10.2.1 Proses pengambilan keputusan Firewall 221
10.2.2 Mengenali algoritma dan aturan Firewall 222
10.3 Konfigurasi dan Pengaturan Firewall 224
10.3.1 Bagaimana menetapkan aturan pada Firewall 225
10.3.2 Kebijakan keamanan dan penerapannya dalam Firewall 227
10.4 Manajemen dan Pemeliharaan Firewall 228
10.4.1 Pembaruan dan peningkatan Firewall 229
10.4.2 Pengawasan dan laporan Firewall 230
10.5 Keamanan dan Firewall: Tantangan dan Solusi 231
10.5.1 Ancaman keamanan yang dapat dicegah dengan Firewall 231
10.5.2 Keterbatasan dan kelemahan Firewall 233
10.5.3 Teknologi dan pendekatan baru dalam Firewall 234
10.6 Kasus Studi: Firewall dalam Praktek 236
10.6.1 Penggunaan Firewall dalam bisnis 236
10.6.2 Penggunaan Firewall dalam pemerintahan 239
10.6.3 Penggunaan Firewall dalam sektor pendidikan 241
10.7 Penutup 241
DAFTAR PUSTAKA 243

BAB 11 INTRUSION DETECTION SYSTEM 245
11.1 Pendahuluan 245
11.2 Perbedaan IDS dan Firewall 246
11.3 Intrusion Detection System (IDS) 247
11.4 Kategori Serangan IDS 249
11.4.1 Misuse detection 249
11.4.2 Anomaly Detection 249
11.4.3 Hybrid Detection 250
11.5 Host Intrusion Detection System (HIDS) 253
11.6 Network Intrusion Detection System 255
11.7 Intrusion Detection System tools by Type Operating System 257
DAFTAR PUSTAKA 259
BAB 12 ADHOC NETWORKING 261
12.1 Pendahuluan 261
12.2 Pengertian Adhoc Networking 261
12.3 Keamanan Adhoc Networking 262
12.4 Ancaman Keamanan Pada Ahoc Networking 263
12.5 Teknik Keamanan Pada Adhoc Networking 265
12.6 Protokol Keamanan 266
12.7 WEP (Wired Equivalent Privacy) 267
12.8 WPA (Wi-fi Protected Acces) 267
12.9 WPA2 (Wi-fi Protected Acces 2) 268
12.10 Manajemen Keamanan Pada Adhoc Networking 269
12.11 Manajemen Identitas 270
12.12 Manajemen Akses 271
12.13 Manajemen Sertifikat 272
12.14 Studi Kasus : Keamanan Adhoc Networking Pada Lingkungan Perusahaan 273
12.15 Analisis Risiko 275
12.16 Implementasi Keamanan Pada Adhoc Networking 276
12.17 Evaluasi Keamanan Pada Adhoc Networking 277
DAFTAR PUSTAKA 279

BAB 13 MOBILE ADHOC NETWORKING 281
13.1 Mobile Ad Hoc Networking (MANET) 281
13.2 Karakteristik MANET 282
13.3 Protokol Routing pada MANET 284
13.4 Protokol DSDV 286
13.5 Protokol DSR 290
13.6 Protokol ZRP 292
DAFTAR PUSTAKA 296
BIODATA PENULIS

DAFTAR GAMBAR

Gambar 1.1. Kemanan Informasi 1
Gambar 1.2. History Icon 7
Gambar 1.3. Keamanan IoT Icon 9
Gambar 1.4. Blockchain Security Icon 12
Gambar 1.5. Quantum Security Icon 14
Gambar 1.6. Icon Penjaga Keamanan 16
Gambar 1.7. US Logo 19
Gambar 1.8. Logo BIN 22
Gambar 1.9. Logo LAMSANEG 23
Gambar 1.10. Logo BSSN 23
Gambar 1.11. Logo Aptika 24
Gambar 1.12. Logo Kemhan 24
Gambar 1.13. Logo BAKAMLA 25
Gambar 2.1. (a), (b) Langkah-langkah enkripsi dan dekripsi 31
Gambar 2.2. Proses steganografi 33
Gambar 3.1. Cara kerja kunci kriptografi simetris 49
Gambar 3.2. Kotak -S AES 51
Gambar 4.1. Diagram alur alur kerja kriptografi 58
Gambar 4.2. Cara kerja kunci kriptografi asymmetric 59
Gambar 4.3. Menggunakan kriptografi kunci publik untuk pertukaran kunci 61
Gambar 8.1. Pengenalan Website 122
Gambar 8.1. Ilustrasi Hosting 130
Gambar 8.2. Cara Hacker Melakukan Serangan SQL Injection 135
Gambar 8.3. Cara Kerja Seranggan XSS 138
Gambar 8.4. Cara Kerja Serangan Cross-Site Request Forgery (CSRF) 141
Gambar 8.5. Cara Kerja Serangan DDoS (*Distributed Denial of Service*) 144

Gambar 8.6. Serangan Brute Force 148
Gambar 8.7. Cara Kerja Attacker Menggunakan Serangan *Man-in-the-Middle* (MitM) 152
Gambar 8.8. Langkah-langkah Serangan Pharming 156
Gambar 8.9. Ilustrasi Serangan File Inclusion 159
Gambar 8.10. Serangan *Server Side Request Forgery* (SSRF) 162
Gambar 8.11. Cara Kerja Serangan Clickjacking 165
Gambar 10.1. Arsitektur Firewall Tunggal 219
Gambar 10.2. Arsitektur Dual Firewall 220
Gambar 11.1. Statistik Aduan Serangan Cyber di Indonesia 246
Gambar 11.2. Cara Kerja Firewall 247
Gambar 11.3. Cara Kerja IDS 248
Gambar 11.4. Arsitektur *Hybrid Detection* 250
Gambar 11.5. Strukur rules untuk IDS 253
Gambar 11.3. Blok Diagram IDS 254
Gambar 11.4. Topologi NIDS 256
Gambar 13.1. Ilustrasi konektivitas jaringan MANET 282
Gambar 13.2. Topologi MANET 283
Gambar 13.3. Algoritma SPF (*Short Path First*), sebuah pendekatan protocol routing 285
Gambar 13.4. Ilustrasi Mekanisme Protokol DSDV 289
Gambar 13.5. Penjelajahan rute Protokol DSR 291
Gambar 13.6. Penjelajahan Rute Zone pada Protokol ZRP 294

DAFTAR TABEL

Tabel 3.1. Transisi Enkripsi Ditentukan dalam NIST SP800-131A, Menunjukkan Masa Hidup Terbatas untuk Sistem Kripto 47
Tabel 10.1. Tabel Aturan Firewall 228
Tabel 10.2. Tabel Aturan Firewall pada PT. XYZ dengan format IPTables 249
Tabel 11.1. Jenis-Jenis Sistem Operasi yang Mendukung HIDS dan NIDS. 257

BAB 1
SEJARAH DAN INTRODUCTION KEAMANAN INFORMASI

Oleh Angga Aditya Permana

1.1 Pendahuluan

Gambar 1.1. Kemanan Informasi

Keamanan informasi mengacu pada praktik dan langkah-langkah yang diambil untuk melindungi informasi dari akses, penggunaan, perubahan, atau pengungkapan yang tidak sah. Hal ini penting untuk memastikan bahwa informasi sensitif dan bernilai, seperti data pribadi, data bisnis, atau rahasia perusahaan, tetap aman dari ancaman internal dan eksternal. Berikut ini adalah penjelasan detail tentang keamanan informasi: (Rahardjo, 2017)

1. Identifikasi dan Klasifikasi Informasi: Langkah pertama dalam keamanan informasi adalah mengidentifikasi dan mengklasifikasikan informasi yang ada. Ini membantu dalam menentukan tingkat keamanan yang tepat untuk setiap jenis informasi. Informasi dapat diklasifikasikan sebagai terbatas, rahasia, atau sangat rahasia berdasarkan tingkat kepekaan dan nilai informasi tersebut.
2. Akses Pengendalian: Keamanan informasi melibatkan pengendalian akses yang ketat terhadap informasi sensitif. Ini dapat dicapai melalui penerapan kebijakan otentikasi, seperti penggunaan kata sandi yang kuat, autentikasi dua faktor, atau biometrik. Selain itu, hak akses pengguna harus dikonfigurasi secara tepat sehingga setiap pengguna hanya memiliki akses ke informasi yang diperlukan untuk menjalankan tugas mereka.
3. Pengendalian Fisik: Keamanan informasi juga mencakup langkah-langkah pengendalian fisik untuk melindungi aset informasi. Ini termasuk penggunaan gembok, kartu akses, sistem pengawasan CCTV, dan pengamanan area fisik yang menyimpan server atau perangkat penyimpanan data. Langkah-langkah ini mencegah akses fisik yang tidak sah ke sistem dan infrastruktur yang menyimpan informasi sensitif.
4. Enkripsi: Enkripsi adalah proses mengubah informasi menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang tepat. Penggunaan enkripsi melindungi informasi saat berada dalam transit atau saat disimpan dalam penyimpanan. Ini membantu mencegah akses yang tidak sah dan melindungi informasi jika perangkat atau data dicuri atau hilang.
5. Pengendalian Jaringan: Jaringan komputer harus dilindungi dengan pengendalian akses yang tepat dan kebijakan keamanan yang kuat. Ini melibatkan penggunaan firewall,

sistem deteksi intrusi, dan protokol keamanan jaringan seperti *Virtual Private Network* (VPN) untuk mengamankan komunikasi jarak jauh. Jaringan juga harus diperbarui secara teratur dengan patch keamanan dan perangkat lunak terbaru untuk mengatasi kerentanan yang diketahui.

6. Pelatihan dan Kesadaran Pengguna: Salah satu aspek penting dari keamanan informasi adalah melibatkan pengguna. Pelatihan keamanan yang tepat harus diberikan kepada semua pengguna untuk memastikan bahwa mereka memahami praktik keamanan, seperti menghindari membuka lampiran email yang mencurigakan, tidak berbagi kata sandi dengan orang lain, atau menghindari mengklik tautan yang mencurigakan. Kesadaran pengguna yang baik dapat membantu mencegah serangan sosial dan kebocoran informasi yang disebabkan oleh kesalahan manusia.
7. Keamanan Fisik dan Kebakaran: Selain pengendalian akses dan kebijakan keamanan teknis, langkah-langkah keamanan fisik seperti kebakaran, banjir, dan proteksi terhadap bencana alam juga penting. Ini termasuk penggunaan pemadam api, sistem deteksi kebakaran, backup data reguler, dan perencanaan pemulihan bencana untuk memastikan bahwa informasi dapat dipulihkan dan tidak hilang akibat kejadian tak terduga.
8. Pengawasan dan Audit: Pengawasan dan audit sistematis diperlukan untuk memastikan kepatuhan terhadap kebijakan keamanan dan mendeteksi aktivitas mencurigakan atau pelanggaran keamanan. Pengawasan melibatkan pemantauan sistem, pemantauan jaringan, analisis log, dan inspeksi rutin untuk mengidentifikasi ancaman potensial atau upaya tidak sah dalam mengakses informasi.

9. Penanggapan Kejadian Keamanan: Organisasi harus memiliki rencana respons kejadian keamanan yang baik yang mencakup tindakan untuk ditindaklanjuti dalam kasus pelanggaran keamanan atau insiden yang terkait. Hal ini mencakup langkah-langkah untuk membatasi kerusakan, mengisolasi sistem yang terkena dampak, mengumpulkan bukti, mengoreksi kerentanan, dan memberikan pemberitahuan kepada pihak yang terkena dampak.
10. Kepatuhan dan Standar: Organisasi harus memastikan bahwa mereka mematuhi peraturan dan standar keamanan informasi yang berlaku di wilayah atau industri mereka. Contohnya adalah Standar Keamanan Data Kartu Pembayaran (PCI DSS) untuk perusahaan yang memproses kartu kredit, atau Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa yang melindungi data pribadi. Kepatuhan terhadap standar ini penting untuk menjaga kepercayaan pelanggan dan meminimalkan risiko hukum.

Demikianlah penjelasan detail tentang keamanan informasi. Penting untuk diingat bahwa praktik keamanan informasi harus terus diperbarui dan disesuaikan dengan ancaman baru yang muncul, serta selalu mengikuti perkembangan teknologi dan tren keamanan terbaru.

Keamanan informasi melibatkan perlindungan data, sistem, dan infrastruktur informasi dari ancaman dan serangan yang dapat mengakibatkan kerugian, kerusakan, atau kehilangan data. Berikut adalah beberapa aspek yang terkait dengan keamanan informasi: (Sulistyowati S.Kom., M.MT., 2021)

1. **Kerahasiaan (*Confidentiality*)**: Kerahasiaan mengacu pada perlindungan informasi agar hanya dapat diakses oleh orang yang berwenang. Ini melibatkan penggunaan

enkripsi, pengaturan izin akses, dan pengamanan fisik untuk mencegah akses yang tidak sah.

2. **Integritas (*Integrity*)**: Integritas berarti memastikan bahwa data dan sistem tetap utuh, tidak diubah secara tidak sah atau tidak sah. Hal ini dapat dicapai dengan menggunakan tanda tangan digital, kontrol versi, dan pemeriksaan periodik terhadap integritas data.
3. **Ketersediaan (*Availability*)**: Ketersediaan berarti memastikan bahwa sistem dan data dapat diakses oleh pengguna yang sah ketika diperlukan. Langkah-langkah seperti redundansi, backup, dan pemulihan bencana diimplementasikan untuk mencegah gangguan layanan dan pemulihan cepat jika terjadi kegagalan.
4. **Keutuhan (*Authenticity*)**: Keutuhan melibatkan memastikan bahwa data dan sumber informasi dapat dipercaya dan benar-benar mewakili apa yang mereka klaim. Ini dapat dicapai dengan menggunakan tanda tangan digital, sertifikat digital, dan metode otentikasi lainnya.
5. **Nonrepudiasi (*Non-repudiation*)**: Nonrepudiasi memastikan bahwa pihak yang terlibat dalam sebuah transaksi atau komunikasi tidak dapat menyangkal keterlibatannya dalam kejadian tersebut. Ini dicapai dengan menggunakan tanda tangan digital dan metode otentikasi yang kuat.
6. **Pengamanan Fisik**: Pengamanan fisik melibatkan perlindungan fisik terhadap perangkat keras, server, dan fasilitas yang menyimpan atau memproses data sensitif. Ini termasuk penggunaan kunci akses, pengawasan akses fisik, dan tindakan keamanan lainnya untuk melindungi aset fisik.
7. **Pengamanan Jaringan**: Pengamanan jaringan melibatkan langkah-langkah untuk melindungi jaringan komputer dari ancaman seperti serangan DDoS, serangan malware, atau

pencurian data. Ini melibatkan penggunaan firewall, deteksi intrusi, enkripsi data, dan pengelolaan akses jaringan.

8. **Keamanan Perangkat Lunak**: Keamanan perangkat lunak melibatkan mengidentifikasi, mencegah, dan memperbaiki kerentanan dalam perangkat lunak. Ini melibatkan penerapan praktik pengembangan yang aman, pemantauan dan pembaruan rutin, serta pengujian keamanan perangkat lunak.
9. **Kesadaran dan Pelatihan**: Kesadaran keamanan informasi dan pelatihan yang tepat bagi pengguna sangat penting. Ini termasuk memberikan pelatihan tentang praktik keamanan, kebijakan keamanan, dan mengajarkan pengguna untuk mengenali dan melaporkan ancaman keamanan.
10. **Kepatuhan dan Regulasi**: Kepatuhan terhadap kebijakan keamanan informasi dan peraturan terkait penting untuk menjaga keamanan informasi. Mengikuti standar keamanan seperti ISO 27001 dan kepatuhan terhadap peraturan privasi data, seperti GDPR, merupakan langkah penting dalam melindungi informasi.
11. **Manajemen Kejadian Keamanan**: Manajemen kejadian keamanan melibatkan mendeteksi, menginvestigasi, dan merespons insiden keamanan. Ini melibatkan pemantauan dan analisis log keamanan, respons terhadap serangan, serta pemulihan dan perbaikan setelah terjadinya insiden.
12. **Pengujian Keamanan (*Security Testing*)**: Pengujian keamanan, seperti uji penetrasi dan audit keamanan, dilakukan untuk mengidentifikasi kerentanan dan celah keamanan yang mungkin ada dalam sistem, aplikasi, atau infrastruktur.

Setiap organisasi harus mengadopsi pendekatan holistik terhadap keamanan informasi, menggabungkan teknologi, kebijakan, dan praktik terbaik untuk melindungi data dan sistem mereka dari ancaman dan serangan.

1.2 Sejarah Keamanan Informasi

Gambar 1.2. History Icon

Sejarah keamanan informasi dimulai seiring dengan perkembangan komunikasi dan pertukaran informasi dalam bentuk elektronik. Berikut ini adalah beberapa peristiwa penting dalam sejarah keamanan informasi: (Rahardjo, 2017)

1. Kriptografi Kuno: Prinsip kriptografi, yang melibatkan penggunaan teknik pengacakan dan penyandian pesan, telah ada sejak zaman kuno. Salah satu contoh kriptografi kuno yang terkenal adalah Sandi Caesar, yang digunakan oleh Julius Caesar untuk mengamankan pesan militer pada abad pertama SM.
2. Kriptografi Selama Perang Dunia: Perang Dunia I dan II mendorong perkembangan teknik kriptografi yang lebih canggih. Selama Perang Dunia II, mesin Enigma yang digunakan oleh Jerman untuk menyandikan komunikasi

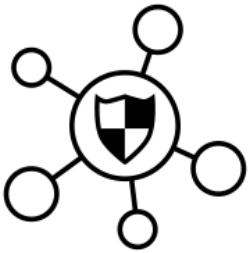
mereka dipecahkan oleh sekelompok matematikawan dan kriptolog dari Inggris, yang terkenal dengan nama "Hut 8" di Bletchley Park.

3. Era Komputer: Dengan munculnya komputer dan teknologi digital pada tahun 1940-an, keamanan informasi menjadi semakin penting. Pada tahun 1970-an, Algoritma Enkripsi Data (DES) dikembangkan sebagai standar enkripsi untuk melindungi komunikasi data pemerintah Amerika Serikat. Namun, kemudian dianggap terlalu lemah karena panjang kunci yang pendek.
4. Kriptografi Kunci Publik: Pada tahun 1970-an, Martin Hellman, Whitfield Diffie, dan Ralph Merkle mengusulkan konsep kriptografi kunci publik. Konsep ini memungkinkan penggunaan dua kunci yang berbeda (kunci publik dan kunci privat) untuk enkripsi dan dekripsi. Ini membuka jalan bagi pengembangan protokol seperti RSA (*Rivest-Shamir-Adleman*) yang masih banyak digunakan hingga saat ini.
5. Internet dan Perlindungan Data: Dengan munculnya Internet pada tahun 1990-an, perlindungan data dan keamanan informasi menjadi lebih penting. Protokol keamanan seperti *Secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS) dikembangkan untuk mengamankan komunikasi online, terutama dalam transaksi e-commerce.
6. Serangan Siber Terkenal: Seiring dengan perkembangan teknologi, serangan siber juga meningkat. Beberapa serangan terkenal termasuk serangan DDoS terhadap situs web seperti Yahoo dan Amazon pada tahun 2000, serangan malware WannaCry pada tahun 2017 yang menyerang ribuan komputer di seluruh dunia, dan serangan peretasan Equifax pada tahun 2017 yang mengakibatkan pencurian data pribadi jutaan orang.

7. Regulasi Perlindungan Data: Kesadaran akan pentingnya keamanan informasi semakin meningkat, dan pemerintah di berbagai negara mulai menerapkan regulasi dan undang-undang perlindungan data. Contohnya adalah Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa yang mulai berlaku pada tahun 2018, yang mengatur bagaimana data pribadi harus dikelola dan dilindungi.
8. Perkembangan Keamanan Cloud dan Kecerdasan Buatan: Dengan semakin luasnya penggunaan layanan cloud dan adopsi kecerdasan buatan, keamanan informasi terus berkembang. Keamanan cloud, seperti enkripsi end-to-end dan pengelolaan akses yang lebih baik, menjadi fokus utama. Sementara itu, kecerdasan buatan digunakan untuk mendeteksi ancaman siber secara otomatis dan meningkatkan respons kejadian keamanan.

Sejarah keamanan informasi terus berkembang seiring dengan perubahan teknologi dan ancaman yang berkembang. Perkembangan terbaru seperti keamanan Internet of Things (IoT), blockchain, dan keamanan quantum juga menjadi fokus penelitian dan pengembangan dalam upaya melindungi informasi di dunia digital yang terus berkembang.

1.3 Keamanan Internet of Things (IoT)



Gambar 1.3. Keamanan IoT Icon

Keamanan *Internet of Things* (IoT) merupakan aspek yang sangat penting dalam ekosistem IoT yang terus berkembang. IoT merujuk pada jaringan perangkat fisik yang terhubung melalui internet dan saling berkomunikasi untuk mengumpulkan dan berbagi data. Beberapa langkah penting dalam menjaga keamanan IoT adalah sebagai berikut:

1. Keamanan Perangkat: Perangkat IoT harus dilindungi dari serangan fisik dan elektronik. Ini melibatkan penggunaan otentikasi kuat, seperti kata sandi unik atau kunci enkripsi, untuk mengamankan akses ke perangkat. Selain itu, penggunaan perangkat keras dan perangkat lunak yang tahan terhadap serangan, serta pembaruan perangkat lunak secara teratur untuk memperbaiki kerentanan yang diketahui, juga penting.
2. Enkripsi dan Privasi Data: Data yang dikirimkan dan diterima oleh perangkat IoT harus dienkripsi untuk melindungi privasi dan mencegah pengungkapan yang tidak sah. Enkripsi end-to-end harus diterapkan, baik saat data sedang ditransmisikan melalui jaringan maupun saat disimpan dalam penyimpanan.
3. Pengelolaan Identitas dan Akses: Pengelolaan identitas dan akses yang tepat diperlukan untuk mengendalikan siapa yang memiliki akses ke perangkat IoT dan data yang dihasilkan. Ini melibatkan penerapan kebijakan otentikasi yang kuat, autentikasi dua faktor, dan manajemen hak akses yang diperlukan untuk setiap perangkat dan pengguna.
4. Jaringan yang Aman: Jaringan tempat perangkat IoT terhubung harus dijaga keamanannya. Ini meliputi penggunaan firewall, enkripsi Wi-Fi, dan penerapan protokol keamanan seperti *Transport Layer Security* (TLS) untuk melindungi komunikasi antara perangkat dan server.

5. Deteksi dan Respon Terhadap Serangan: Sistem yang dapat mendeteksi dan merespons serangan terhadap perangkat IoT sangat penting. Ini melibatkan penggunaan teknologi deteksi intrusi yang canggih, analisis perilaku, dan pemantauan yang terus-menerus untuk mengidentifikasi aktivitas mencurigakan atau ancaman potensial.
6. Pembaruan dan Pemulihan: Perangkat IoT harus memiliki kemampuan untuk menerima pembaruan perangkat lunak secara teratur guna mengatasi kerentanan keamanan yang baru ditemukan. Selain itu, rencana pemulihan bencana dan cadangan data harus ada untuk memulihkan sistem jika terjadi serangan atau kegagalan perangkat.
7. Kesadaran Pengguna: Kesadaran dan pelatihan pengguna sangat penting dalam keamanan IoT. Pengguna harus diberikan informasi tentang ancaman keamanan dan praktik terbaik dalam menggunakan dan mengelola perangkat IoT. Ini termasuk memperbarui kata sandi secara teratur, memeriksa sertifikat keamanan, dan melaporkan aktivitas mencurigakan.
8. Standar dan Regulasi: Standar dan regulasi keamanan IoT yang dikeluarkan oleh lembaga standar dan pemerintah berperan penting dalam menjaga keamanan IoT secara keseluruhan. Mereka mempromosikan praktik keamanan yang konsisten, melindungi privasi pengguna, dan mendorong produsen untuk mengembangkan produk yang aman.

Keamanan IoT merupakan tantangan yang kompleks karena melibatkan jaringan yang luas dan beragam perangkat. Oleh karena itu, penting untuk menerapkan pendekatan yang holistik dan terus-menerus memperbarui keamanan IoT dengan mempertimbangkan perkembangan teknologi dan ancaman yang berkembang.

1.4 Keamanan Blockchain

Gambar 1.4. Blockchain Security Icon

Keamanan blockchain adalah aspek kunci dalam menjaga integritas dan keandalan teknologi blockchain. Berikut adalah beberapa aspek penting dalam keamanan blockchain:

1. Kriptografi: Blockchain menggunakan teknik kriptografi untuk mengamankan data dan transaksi. Kunci publik dan kunci privat digunakan dalam enkripsi dan dekripsi data. Algoritma hash kriptografis seperti SHA-256 digunakan untuk menghasilkan tanda tangan digital yang unik dan mengamankan integritas data.
2. Desentralisasi: Keamanan blockchain bergantung pada sifat desentralisasinya. Blockchain didistribusikan di seluruh jaringan komputer yang disebut "node". Setiap node memiliki salinan lengkap dari blockchain dan secara kolektif memverifikasi dan memvalidasi transaksi. Ini mencegah serangan satu titik kegagalan dan menjaga keandalan sistem.
3. Konsensus: Blockchain menggunakan mekanisme konsensus untuk memastikan bahwa semua node dalam jaringan setuju tentang status yang benar dari blockchain. Mekanisme konsensus seperti *Proof of Work* (PoW) atau

Proof of Stake (PoS) memastikan bahwa hanya transaksi yang valid yang dimasukkan ke dalam blockchain. Mekanisme ini juga melindungi terhadap serangan dengan membutuhkan upaya komputasi yang signifikan atau kepemilikan aset kripto yang cukup untuk mempengaruhi proses konsensus.

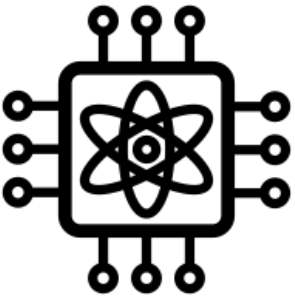
4. Struktur Data Terhubung (*Linked Data Structure*): Blockchain menggunakan struktur data terhubung dengan blok yang saling terkait. Setiap blok berisi hash dari blok sebelumnya, membentuk rantai yang tidak bisa diubah. Ini membuatnya sangat sulit untuk mengubah data yang ada di blockchain, karena akan memerlukan modifikasi pada semua blok yang terkait, serta upaya komputasi yang besar.
5. Verifikasi Transparan: Keamanan blockchain juga terkait dengan transparansinya. Semua transaksi yang dimasukkan ke dalam blockchain dapat dilihat oleh semua peserta jaringan. Ini memungkinkan verifikasi independen dari transaksi dan mencegah manipulasi data yang tidak terdeteksi.
6. Keamanan Jaringan: Keamanan jaringan sangat penting dalam melindungi blockchain. Protokol keamanan seperti *Transport Layer Security* (TLS) dan enkripsi data harus diterapkan untuk melindungi komunikasi antara node dalam jaringan. Jaringan juga harus dilindungi dari serangan jaringan seperti serangan DDoS atau serangan 51%.
7. Audit dan Pemantauan: Sistem blockchain harus memiliki mekanisme audit dan pemantauan yang efektif. Ini melibatkan pemantauan aktivitas jaringan, analisis transaksi, dan deteksi dini terhadap serangan atau perilaku mencurigakan. Tim keamanan harus terus memperbarui

dan memperbaiki keamanan sistem sesuai dengan perkembangan terbaru dalam teknologi dan ancaman.

8. *Smart Contract Security*: *Smart contract* dalam blockchain, seperti pada platform Ethereum, juga membutuhkan perhatian keamanan yang serius. Kontrak pintar yang tidak aman dapat disalahgunakan untuk mencuri aset digital atau mengeksekusi kode berbahaya. Pemeriksaan kode dan audit keamanan harus dilakukan secara teratur untuk memastikan kontrak pintar bebas dari kerentanan dan serangan.

Keamanan blockchain adalah aspek yang penting untuk mendapatkan kepercayaan pengguna dan menjaga integritas data. Terus-menerus memperbarui dan meningkatkan praktik keamanan serta beradaptasi dengan ancaman baru adalah penting untuk memastikan sistem blockchain tetap aman dan andal.

1.5 Keamanan Quantum



Gambar 1.5. Quantum Security Icon

Keamanan quantum adalah bidang keamanan informasi yang berkaitan dengan ancaman dan perlindungan terhadap komputasi kuat yang mungkin disediakan oleh komputer kuantum. Keamanan informasi saat ini didasarkan pada asumsi-asumsi

matematis terkait dengan kompleksitas komputasi klasik. Namun, komputer kuantum memiliki kemampuan potensial untuk memecahkan beberapa masalah yang saat ini dianggap sulit atau tidak mungkin bagi komputer klasik.

Berikut ini adalah beberapa aspek penting dalam keamanan quantum:

1. Kriptografi Kuantum: Kriptografi kuantum adalah salah satu cabang utama keamanan quantum. Ini melibatkan pengembangan protokol dan algoritma kriptografi yang dapat menahan serangan dari komputer kuantum. Misalnya, algoritma enkripsi kunci publik yang aman terhadap serangan komputer kuantum, seperti Algoritma Kunci Publik Kuantum (*Quantum Key Distribution* - QKD), telah dikembangkan.
2. Komputasi Kuantum-aman: Keamanan komputasi kuantum-aman melibatkan pengembangan algoritma dan protokol yang tidak rentan terhadap serangan komputer kuantum. Ini melibatkan penggunaan algoritma yang kuat dan metode enkripsi yang tahan terhadap serangan komputasi kuantum, seperti Homomorfik Enkripsi Kuantum.
3. Post-Kriptografi Kuantum: Keamanan informasi saat ini sangat bergantung pada algoritma kriptografi klasik. Namun, komputer kuantum dapat memecahkan beberapa algoritma tersebut dengan cepat. Oleh karena itu, diperlukan pengembangan algoritma baru yang tahan terhadap serangan komputer kuantum. Bidang ini dikenal sebagai post-kriptografi kuantum, yang mencoba mengembangkan sistem kriptografi yang dapat bertahan dalam era komputasi kuantum.
4. Perlindungan Data Kuantum: Keamanan data dalam komunikasi kuantum menjadi penting. Protokol komunikasi kuantum, seperti QKD, memungkinkan

pertukaran kunci kriptografi yang aman melalui saluran yang tidak dapat disadap. Selain itu, mekanisme deteksi pengawasan dalam sistem komunikasi kuantum dapat mendeteksi upaya peretasan atau intersepsi pada data.

5. Riset dan Standar: Keamanan quantum merupakan area penelitian yang aktif dan terus berkembang. Organisasi standar seperti *National Institute of Standards and Technology* (NIST) sedang mengadakan kompetisi untuk mengembangkan algoritma kriptografi kuantum-aman baru. Standar keamanan quantum yang dapat diterima secara internasional akan menjadi penting untuk memastikan bahwa sistem dan infrastruktur dapat dilindungi dengan baik di era komputasi kuantum.

Dalam menghadapi era komputasi kuantum, banyak upaya sedang dilakukan untuk mengembangkan solusi keamanan quantum yang tahan terhadap serangan komputer kuantum. Perkembangan dalam bidang ini terus berlangsung, dan kolaborasi antara komunitas keamanan informasi, ilmu komputer, dan fisika kuantum sangat penting untuk menghadapi tantangan keamanan yang dibawa oleh teknologi komputasi kuantum.

1.6 Orang yang Terlibat dalam Keamanan Informasi

Gambar 1.6. Icon Penjaga Keamanan

Ada beberapa peran dan jenis orang yang terlibat dalam bidang keamanan informasi. Berikut adalah beberapa contoh orang yang terlibat dalam keamanan informasi:

1. Kepala Keamanan Informasi (*Chief Information Security Officer* - CISO): CISO adalah individu yang bertanggung jawab atas strategi, kebijakan, dan pelaksanaan keamanan informasi dalam organisasi. Mereka mengawasi fungsi keamanan informasi dan memastikan perlindungan data dan sistem secara menyeluruh.
2. Analis Keamanan Informasi: Para analis keamanan informasi adalah ahli yang menganalisis risiko keamanan dan serangan potensial terhadap sistem dan infrastruktur. Mereka melakukan penilaian keamanan, mengidentifikasi kerentanan, dan merancang solusi keamanan yang efektif.
3. Insinyur Keamanan: Insinyur keamanan adalah individu yang terlibat dalam merancang, mengimplementasikan, dan memelihara infrastruktur keamanan. Mereka bekerja dengan tim pengembangan dan jaringan untuk memastikan bahwa sistem, perangkat lunak, dan jaringan dirancang dengan prinsip keamanan yang kuat.
4. Penetration Tester: Penetration tester (*ethical hacker*) adalah orang yang melaksanakan serangan simulasi terhadap sistem dan aplikasi untuk mengidentifikasi kerentanan dan celah keamanan. Mereka melakukan uji penetrasi untuk mengevaluasi kekuatan sistem dan memberikan rekomendasi perbaikan.
5. Administrator Keamanan Jaringan: Administrator keamanan jaringan bertanggung jawab atas pengelolaan keamanan jaringan dan sistem. Mereka mengatur konfigurasi jaringan, firewall, dan perangkat keamanan lainnya serta memantau dan merespons ancaman keamanan.

6. Analis Kejadian Keamanan: Analis kejadian keamanan memantau dan menganalisis aktivitas jaringan dan sistem untuk mendeteksi insiden keamanan. Mereka mengevaluasi log dan jejak aktivitas, mengidentifikasi serangan, dan memberikan respons dan pemulihan yang tepat.
7. Manajer Kebijakan Keamanan: Manajer kebijakan keamanan bertanggung jawab untuk merancang, mengimplementasikan, dan memantau kebijakan dan prosedur keamanan organisasi. Mereka memastikan kepatuhan terhadap standar keamanan yang berlaku dan memperbarui kebijakan sesuai dengan ancaman dan perubahan teknologi.
8. Konsultan Keamanan: Konsultan keamanan adalah individu atau tim yang menyediakan layanan konsultasi keamanan kepada organisasi. Mereka membantu dalam menganalisis risiko, merancang strategi keamanan, melakukan audit keamanan, dan memberikan saran untuk memperkuat keamanan informasi.
9. Pelatih Keamanan Informasi: Pelatih keamanan informasi bertanggung jawab untuk memberikan pelatihan dan kesadaran kepada pengguna tentang praktik keamanan yang baik. Mereka menyampaikan pengetahuan tentang risiko keamanan, taktik serangan, dan langkah-langkah pencegahan yang diperlukan.
10. Penegak Hukum dan Penyelidik: Penegak hukum dan penyelidik berperan dalam penegakan hukum dan penanganan kasus kejahatan komputer. Mereka menyelidiki serangan siber, melakukan penuntutan terhadap pelaku kejahatan, dan bekerja sama dengan lembaga penegak hukum untuk menangani kasus-kasus keamanan informasi.

Peran-peran ini mungkin dapat bervariasi tergantung pada organisasi dan lingkungan kerja. Namun, kolaborasi antara berbagai orang dan tim yang terlibat dalam keamanan informasi sangat penting untuk memastikan perlindungan yang kuat dan responsif terhadap ancaman keamanan.

1.7 Badan Keamanan Negara di Dunia

Gambar 1.7. US Logo

Berikut adalah daftar lengkap beberapa badan keamanan informasi terkemuka di dunia beserta detilnya:

1. *National Security Agency* (NSA) - Amerika Serikat:
    a. Tugas: Badan intelijen elektronik yang bertanggung jawab atas pengumpulan dan analisis informasi intelijen asing serta melindungi sistem informasi nasional.
    b. Website: www.nsa.gov

2. *Government Communications Headquarters* (GCHQ) - Britania Raya:
    a. Tugas: Badan intelijen sinyal Britania Raya yang berfokus pada pengumpulan informasi intelijen dan kegiatan siber untuk keamanan nasional.

b. Website: www.gchq.gov.uk

3. *Communications Security Establishment* (CSE) - Kanada:
   a. Tugas: Badan intelijen sinyal Kanada yang bertanggung jawab atas keamanan komunikasi nasional dan kegiatan intelijen sinyal.
   b. Website: www.cse-cst.gc.ca

4. *Australian Signals Directorate* (ASD) - Australia:
   a. Tugas: Badan intelijen sinyal Australia yang bertugas melindungi dan mempertahankan keamanan komunikasi dan sistem informasi nasional.
   b. Website: www.asd.gov.au

5. *Bundesamt für Verfassungsschutz* (BfV) - Jerman:
   a. Tugas: Badan intelijen dalam negeri Jerman yang bertugas melindungi keamanan negara dari ancaman seperti spionase dan terorisme.
   b. Website: www.verfassungsschutz.de

6. *Central Security Service* (CSS) - Amerika Serikat:
   a. Tugas: Badan gabungan antara NSA dan Departemen Pertahanan AS yang bertanggung jawab atas operasi dan keamanan informasi militer AS.
   b. Website: www.nsa.gov/about/cryptologic-centers/css

7. *Cybersecurity and Infrastructure Security Agency* (CISA) - Amerika Serikat:
   a. Tugas: Badan keamanan siber nasional AS yang bertugas melindungi infrastruktur kritis dan mengoordinasikan respons terhadap serangan siber.
   b. Website: www.cisa.gov

8. *National Cyber Security Centre* (NCSC) - Britania Raya:
    a. Tugas: Badan keamanan siber nasional Britania Raya yang bertanggung jawab atas keamanan siber negara dan memberikan nasihat dan bimbingan kepada sektor publik dan swasta.
    b. Website: www.ncsc.gov.uk

9. *Agence nationale de la sécurité des systèmes d'information* (ANSSI) - Prancis:
    a. Tugas: Badan keamanan siber nasional Prancis yang bertugas melindungi sistem informasi negara dari ancaman siber.
    b. Website: www.ssi.gouv.fr

10. *Israel National Cyber Directorate* (INCD) - Israel:
    a. Tugas: Badan keamanan siber nasional Israel yang bertanggung jawab melindungi infrastruktur dan sistem informasi negara dari ancaman siber.
    b. Website: www.gov.il/en/departments/israel_national_cyber_directorate

11. *Cybersecurity Agency of Singapore* (CSA) - Singapura:
    a. Tugas: Badan keamanan siber nasional Singapura yang bertanggung jawab atas keamanan siber negara dan mengembangkan strategi keamanan siber.
    b. Website: www.csa.gov.sg

12. *China National Cybersecurity Agency* (CNCA) - Tiongkok:
    a. Tugas: Badan keamanan siber nasional Tiongkok yang bertugas melindungi infrastruktur siber dan mempertahankan keamanan informasi negara.
    b. Website: www.cac.gov.cn

Perlu diingat bahwa daftar ini hanya mencakup beberapa badan keamanan informasi terkemuka di dunia, dan setiap negara memiliki badan keamanan informasi sendiri dengan peran dan tanggung jawab yang mungkin berbeda-beda.

1.8 Badan Keamanan Negara di Indonesia

Di Indonesia, terdapat beberapa badan keamanan informasi yang berperan dalam menjaga keamanan informasi dan sistem komputer negara. Berikut adalah beberapa badan keamanan informasi di Indonesia:

1. Badan Intelijen Negara (BIN):

Gambar 1.8. Logo BIN

   a. Tugas: Melaksanakan intelijen keamanan nasional, kontra-intelijen, dan penanggulangan terorisme di Indonesia.
   b. Website: www.bin.go.id

2. Lembaga Sandi Negara (LEMSANEG):

Gambar 1.9. Logo LAMSANEG

a. Tugas: Bertanggung jawab atas kebijakan, koordinasi, dan pengawasan dalam bidang sandi negara serta mengembangkan teknologi dan sistem keamanan informasi negara.
b. Website: www.lemsaneg.go.id

3. Badan Siber dan Sandi Negara (BSSN):

Gambar 1.10. Logo BSSN

a. Tugas: Melindungi sistem informasi negara dari serangan siber, mengkoordinasikan upaya perlindungan keamanan siber di Indonesia, serta

memberikan nasihat dan bimbingan dalam bidang keamanan siber.

b. Website: www.bssn.go.id

4. Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika):

Gambar 1.11. Logo Aptika

a. Tugas: Bertanggung jawab atas pengembangan dan pengelolaan aplikasi informatika serta sistem informasi pemerintah.
b. Website: www.aptika.kominfo.go.id

5. Direktorat Jenderal Aplikasi dan Informatika Kementerian Pertahanan (Ditjen Aplikasi dan Informatika Kemhan):

Gambar 1.12. Logo Kemhan

a. Tugas: Mengembangkan dan mengelola aplikasi dan sistem informasi di lingkungan Kementerian Pertahanan.
b. Website: www.kemhan.go.id

6. Pusat Teknologi Informasi dan Komunikasi (Pustekkom):
   a. Tugas: Menyediakan dukungan teknis dan operasional dalam bidang teknologi informasi dan komunikasi untuk lembaga-lembaga pemerintah.
   b. Website: www.pustekkom.kominfo.go.id

7. Badan Keamanan Laut (BAKAMLA):

Gambar 1.13. Logo BAKAMLA

   a. Tugas: Bertanggung jawab atas pengawasan, pengamanan, dan penegakan hukum di wilayah perairan Indonesia, termasuk pengamanan sistem informasi maritim.
   b. Website: www.bakamla.go.id

Peran dan tanggung jawab badan keamanan informasi di Indonesia dapat berbeda-beda, tetapi secara umum, mereka berfokus pada perlindungan sistem informasi negara, keamanan siber, dan perlindungan terhadap ancaman dalam negeri dan luar negeri.

DAFTAR PUSTAKA

Rahardjo, B. 2017. 'Keamanan Informasi & Jaringan', p. 47. Available at: http://budi.rahardjo.id/files/keamanan.pdf.

Sulistyowati S.Kom., M.MT., I. 2021. 'Pengantar Keamanan Sistem Komputer & Jaringan Komputer', pp. 1–46.

BAB 2
PERKENALAN KRIPTOGRAFI

Oleh Nur Hayati

2.1 Sejarah Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu kripto (rahasia) dan graphia (tulisan). Menurut terminologi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (*the art and science of keeping message secure*) (Schneier, 1996). Berbeda dengan kriptografi, kriptanalisis bekerja untuk memecahkan cipherteks.

Pada tahun 3000 SM bangsa Mesir menggunakan teknik *hieroglyphcs* untuk menyembunyikan pesan sehingga tidak dapat terbaca oleh orang lain selain penerima pesan. Kemudian sekitar tahun 50 SM, Julius Caesar menggunakan teknik cipher subtitusi untuk mengirimkan pesan ke Marcus Tullius Cicero. Selanjutnya pada abad ke-9, seorang filsuf Arab Al Kindi menulis risalat yang diberi judul "*A Manuscript on Deciphering Cryptographic Messages*" (Mrayati, Alam and At-Tayyan, 2002). Dimana Al Kindi menemukan teknik untuk memecahkan cipherteks berdasarkan frekuensi kemunculan karakter di dalam pesan yang ada pada Al Quran (Wirdasari, 2008). Teknik ini terkenal dengan nama analisis frekuensi. Kemudian Thomas Jefferson di tahun 1790 membuat alat enkripsi dari 26 disk. Selanjutnya pada tahun 1920 ditemukan mesin kriptografi mekanik "Hagelin Machine" oleh Boris Hagelin di Scockholm, Swedia.

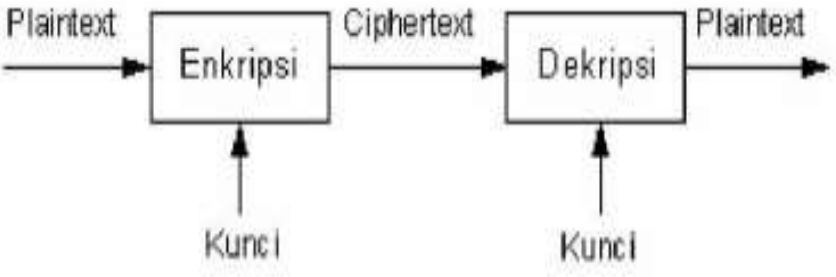
Pada perang dunia ke II, pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan "Enigma". Kemudian pada tahun 1976, Diffie dan Hellman memperkenalkan konsep kunci publik untuk proses pertukaran kunci. Selanjutnya pada awal tahun 1977,

Feistel menemukan algoritma *DES* (*Data Encryption Standard*) yang dipakai untuk mengenkripsi informasi. Setelah itu bermunculan teknik-teknik kriptografi sebagai pengembangan dari teknik sebelumnya hingga saat ini.

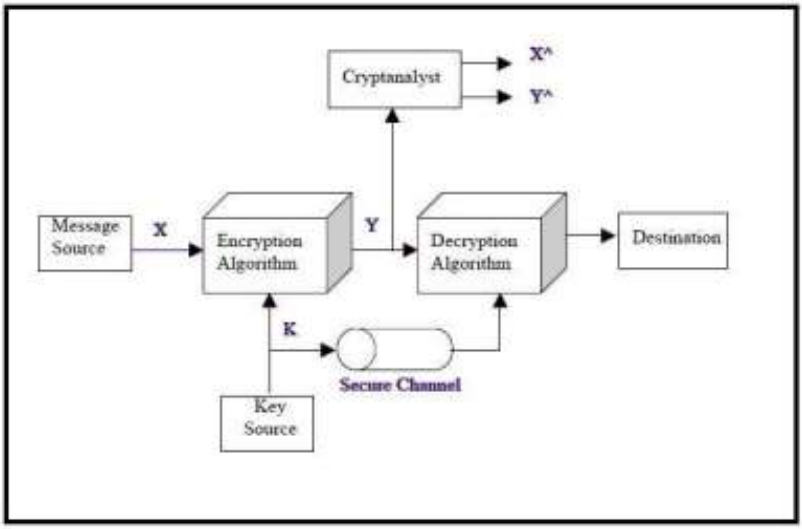
Berikut ini adalah istilah-istilah yang digunakan dalam kriptografi:

1. Plainteks (P) adalah pesan yang akan dikirimkan.
2. Cipherteks (C) adalah pesan terenkrip.
3. Enkripsi (E) adalah proses mengubah bentuk plainteks menjadi cipherteks.
4. Dekrispi (D) adalah proses mengubah bentuk cipherteks menjadi pesan awal (plainteks).
5. Kunci adalah informasi tambahan yang digunakan pada proses enkripsi dan dekripsi.
6. Algoritma kriptografi adalah langkah-langkah disusun sehingga dapat menyembunyikan pesan (dapat berupa fungsi matematis).

Ilustrasi:



(a)



(b)

Gambar 2.1. (a), (b) Langkah-langkah enkripsi dan dekripsi

Gambar 2.1 (a) dan (b) merupakan proses kriptografi enkripsi yang dimulai dari plainteks kemudian berubah menjadi cipherteks dan dekripsi yang mengubah kembali cipherteks menjadi plainteks. Penggunaan kunci dilakukan pada algoritma kriptografi asimetris. Pada gambar 2.1 (b), proses kriptanalisis terjadi pada setelah proses enkripsi selesai dilakukan. Proses kriptanalisis dilakukan untuk mengetahui plainteks tanpa sepengetahuan si pengirim atau mengubah plainteks yang dikirimkan ke penerima pesan, sehingga informasi yang disampaikan tidak sesuai dengan pesan awal si pengirim.

Notasi Matematis:

1. C = chiperteks, P = plainteks
2. Fungsi enkripsi E memetakan P hingga menjadi C
   $E(P) = C$
3. Fungsi dekripsi D memetakan C hingga menjadi P
   $D(C) = P$

4. Proses pengembalian ke pesan asal:
   D(E(P)) = P
5. Jika menggunakan kunci K, maka fungsi enkripsi dan dekripsi menjadi
   EK(P) = C
   DK(C) = P
   dan kedua fungsi ini memenuhi
   DK(EK(P)) = P

Dasar-dasar matematika dari kriptografi terdiri dari *AND, OR, XOR, MOD*, konversi bit ke *Hexa* dan sebaliknya.
Contoh :
P = Besok ketemu di kampus
C = Besokketemudikampus

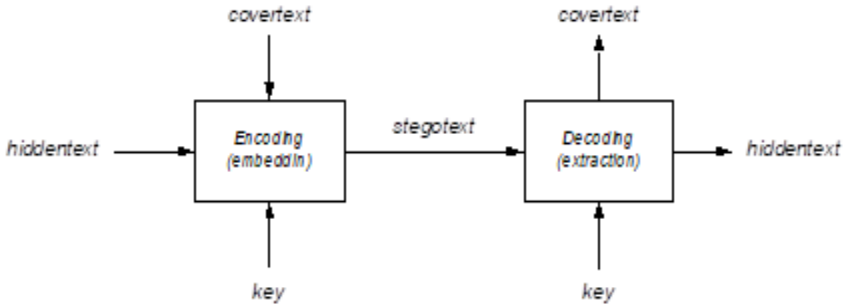
Bentuk dari plainteks dapat berupa teks, gambar, audio maupun video. Bentuk plainteks ke cipherteks dapat berbeda-beda sehingga memungkinkan seseorang tidak dapat memecahkan bentuk dari cipherteks yang sudah dibuat (steganografi). Hasil enkripsi dinilai baik jika cipherteks tidak dapat dengan mudah ditembus oleh seorang kriptanalisis. Akan tetapi, jika kita mau melakukan proses enkripsi, kita juga harus memastikan proses dekripsi dapat dilakukan sehingga jika terjadi sesuatu pada data yang kita enkrip, dapat segera diperbaiki kembali seperti semula.

2.2 Algoritma Kriptografi

Sebelum masuk ke pembahasan mengenai algoritma kriptografi terlebih dahulu kita bahas mengenai steganografi. Steganografi berasal dari bahasa Yunani, steganos (tulisan tersembunyi). Sehingga definisi dari steganografi adalah Tulian tersembunyi dari sebuah cipherteks. Istilah-istilah dalam steganografi terdiri dari:

1. *Hiddentext* adalah pesan tersembunyi
2. *Covertext* adalah pesan atau media yang digunakan untuk menyembunyikan hiddentext
3. *Stegotext* adalah pesan yang sudah berisi pesan hiddentext

Steganografi merupakan pelengkap dari kriptografi bukan sebagai pengganti, fungsinya adalah menyembunyikan keberadaan dari pesan yang sudah dienkripsi pada proses kriptografi (*hiddentext*).
Ilustrasi:



Gambar 2.2. Proses steganografi

Pada gambar 2.2 terlihat bahwa proses steganografi dilakukan setelah proses enkripsi sehingga menghasilkan *hiddentext* yang kemudian dilakukan encoding dengan untuk menghasilkan *covertext* dimana *hiddentext* tersembunyi dalam *covertext* tersebut. Selanjutnya untuk proses menghasilkan kembali *hiddentext* (cipherteks), maka dilakukan *decoding* untuk membuka *covertext* yang sebelumnya menutupi *hiddentext*. Pada proses *steganotext* ini hanya sampai menghasilkan *hiddentext* bukan plainteks.
Beberapa metode staganografi []:

1. Penggunaan tinta yang tidak terlihat atau *invisible ink* (bangsa Romawi).

2. *Pink punctures*, yaitu beberapa tusukan pin-pin kecil pada kertas yang tidak akan kelihatan jika tidak diberikan cahaya terang.
3. Menyembunyikan pesan di dalam sebuah gambar atau foto.
4. Histalaeus, yaitu pesan yang ditato di kepala budak yang telah digunduli.

Ilustrasi:
Staganografi: Bilamana engkau sudah olah kelapa dalam anjungan tadi ambil nampan gulanya
Jawaban: Besok datang

2.2.1 Kriptogradi Klasik

Algoritma kriptografi klasik terbagi menjadi dua yaitu:

1. Cipher subtitusi
   Cipher subtitusi adalah cipher dengan cara mensubtitusi huruf dengan huruf yang lain sesuai dengan aturan yang ditetapkan. Aturan yang ditetapkan tersebut bergantung pada proses enkripsi dan dekripsi.
   Ilustrasi:
   Algoritma: Caesar Cipher
   Lakukan pergeseran 3 langkah ke kanan

Pi	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ci	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

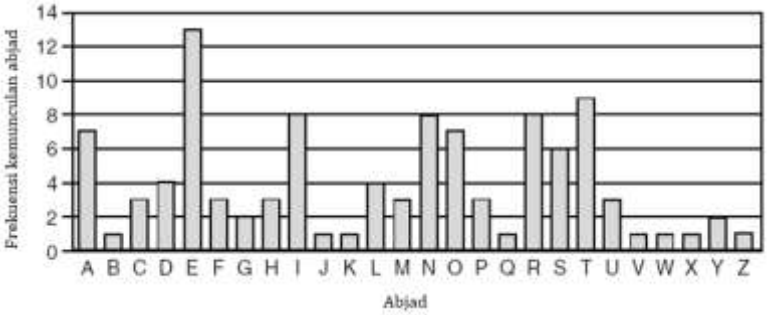
   P = BESOK KETEMU DI DEPAN GERBANG KAMPUS
   C = EHVRN NHWHPX GL GHSDQ JHUEDQJ NDPSXV

   Beberapa varian dalam cipher subtitusi adalah sebagai berikut:
   a. Cipher Subtitusi Abjad-Tunggal (*Monoalphabetic Subtitution Cipher*)
      Yaitu, mengubah satu karakter pada plainteks menjadi satu karakter pada cipherteks dengan aturan tertentu.

Ilustrasi:
P = BESOK KETEMU DI DEPAN GERBANG KAMPUS
Buanglah huruf yang sama pada kalimat di atas, kemudian gantikan dengan huruf yang tidak ada pada kalimat.

BESOK TMU DI PAN GRB S
C = BESOKTMUDIPANGRCFHJLQVWXYZ

b. Cipher Subtitusi Homofonik (*Homofonic Subtitution Cipher*)
Yaitu, teknik untuk meningkatkan kesulitan analisis frekuensi pada cipher subtitusi dalam menyamarkan frekuensi huruf plainteks (Rinaldi, 2006).
Ilustrasi:
Misal diambil sebuah teks dengan frekuensi kemunculan untuk setiap abjad adalah sebagai berikut:



Frekuensi setiap abjad:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	1	3	4	13	3	2	3	7	1	1	4	3	8	7	3	1	8	6	9	3	1	1	1	2	1

Kemudian dipetakan satu-ke-banyak dengan kombinasi cipher bebas.
Misal:
B → AT
C → DL BA AU
Berikut adalah tabel ciphering satu-ke-banyak berdasarkan hasil data frekuensi di atas: (hasil ciphering boleh berbeda)

Huruf Plainteks	**Pilihan untuk unit cipherteks**												
A	BU	CP	AV	AH	BT	BS	CQ						
B	AT												
C	DL	BK	AU										
D	BV	DY	DM	AI									
E	DK	CO	AW	BL	AA	CR	BM	CS	AF	AG	BO	BN	BE
F	BW	CM	CN										
G	DN	BJ											
H	AS	CL	CK										
I	DJ	BI	AX	CJ	AB	BP	CU	CT					
J	BX												
K	DI												
L	AR	BH	CI	AJ									
M	DH	BG	AY										
N	BY	DG	DF	CH	AC	BR	DU	DT					
O	DZ	BF	DX	AK	CG	BQ	DR						
P	BZ	DE	AZ										
Q	DD												
R	AQ	DC	DQ	AL	CE	CF	CV	DS					
S	AP	AN	AO	CD	DW	DV							
T	CB	DB	DP	CC	AD	CY	CW	CX	AE				
U	CA	AM	BA										
V	BB												
W	CZ												
X	BD												
Y	DO	DA											
Z	BC												

Hasil tabel di atas kemudian kita terapkan pada sebuah plainteks. Misal:
P = KRIPTOGRAFI
C = DI DS DJ AZ CB DR DN AQ CQ BW CT

c. Cipher Subtitusi Abjad-Majemuk (*Polyalphabetic Subtitution Cipher*)

Yaitu, teknik pengamanan pesan dengan menggunakan kunci berganda untuk setiap huruf di dalam plainteks.

Ilustrasi:

P = KRIPTO

Kunci = CAESAR

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Perhitungan:

(K + C) *mod* 26 = (11 + 3) *mod* 26 = 14 = (N)

(R + A) *mod* 26 = (18 + 1) *mod* 26 = 19 = (S)

(I + E) *mod* 26 = (9 + 5) *mod* 26 = 14 = (N)

(P + S) *mod* 26 = (16 + 19) *mod* 26 = 35 *mod* 26 = 9 = (I)

(T + A) *mod* 26 = (20 + 1) *mod* 26 = 21 (U)

(O + R) *mod* 26 = (15 + 18) *mod* 26 = 33 *mod* 26 = 7 (G)

C = NSNIUG

d. Cipher Subtitusi Poligram (*Polygram Subtitution Cipher*)

Yaitu, mengenkripsi atau mendekripsi huruf yang dikelompokkan ke dalam beberapa kelompok huruf. Misal AS diganti RT (bigram), IND diganti IOK. Contoh Cipher Poligram adalah *Playfair Cipher*.

Ilustrasi:

Membuat kunci:

Kunci_awal = BESOK KETEMU DI KAMPUS

1) Buang huruf J (jika ada) dan huruf yang berulang.
   BESOK TMU DI PAN GRB S
2) Lalu tambahkan huruf yang belum ada (kecuali J).
   BESOKTMUDIPANGRCFHLQVWXYZ

3) Buat bujur sangkar 5x5 dan susun kunci di dalam bujur sangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

B	E	S	O	K
T	M	U	D	I
P	A	N	G	R
C	F	H	L	Q
V	W	X	Y	Z

B	E	S	O	K	B
T	M	U	D	I	T
P	A	N	G	R	P
C	F	H	L	Q	C
V	W	X	Y	Z	B
B	E	S	O	K	

4) Setelah mendapatkan kunci, tulis pesan dalam pasangan huruf (bigram), jangan sampai ada pasangan huruf yang sama dan hilangkan huruf J. Sisipkan huruf Z pada pasangan huruf yang sama dan jumlah huruf yang ganjil.
   Contoh:
   P = KRIPTO
   menjadi
   KR IP TO
5) Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.
6) Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya.
7) Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

KR = YI

B	E	S	O	K	B
T	M	U	D	**I**	T
P	A	N	G	R	P
C	F	H	L	Q	C
V	W	X	**Y**	Z	B
B	E	S	O	K	

IP = TR

B	E	S	O	K	B
T	M	U	D	I	T
P	A	N	G	R	P
C	F	H	L	Q	C
V	W	X	Y	Z	B
B	E	S	O	K	

TO = DB

B	E	S	O	K	B
T	M	U	D	I	T
P	A	N	G	R	P
C	F	H	L	Q	C
V	W	X	Y	Z	B
B	E	S	O	K	

C = YITRDB

2. Cipher transposisi

   Hasil cipherteks pada algoritma ini diperoleh dengan merubah huruf di dalam plainteks (*transpose*), atau sering disebut sebagai permutasi.

   Ilustrasi:

   P = BESOK BELAJAR KRIPTOGRAFI BERSAMA

   Ubah menjadi:

   BESOK
   BELAJ
   ARKRI
   PTOGR
   AFIBE
   RSAMA

   C = BBAPAR EERTFS SLKOIA OARGNM KJIREA

2.2.2 Kriptografi Modern

Kriptografi modern beroperasi dalam mode bit, dimana plainteks, cipherteks dan kunci dioperasikan dalam rangkaian bit.
Ilustrasi:
P = 011000101001
Dibagi menjadi blok 4-bit:

0110	0010	1001
$0 + 2^2 + 2^1 + 0 = 6$	$0 + 0 + 2^1 + 0 = 2$	$2^3 + 0 + 0 + 2^0 = 9$

Kemudian lakukan proses XOR terhadap kunci 1011

```
0110  0010  1001
1011  1011  1011
⊕
1101  1001  0010
```

Geser 1 bit ke kiri sehingga menjadi:
C = 1011 0010 0101
Macamnya terdiri dari:

1. Algoritma simetris
   Algoritma ini menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Macam-macam algoritma simetris diantaranya adalah *DES*, *AES*, *IDEA*, dan lain-lain.
2. Algoritma asimetris
   Algoritma ini menggunakan kunci publik dan privat untuk proses enkripsi dan dekripsi. Contoh *Rivest, Shamir, Adleman*, *ElGamal, Rabin, Diffie-Hellman Key Exchange, DSA*, dan lain-lain.
3. Algoritma hibrida
   Yaitu, kombinasi antara algoritma simetris dan asimetris.

Sedangkan algoritma yang beroperasi dalam mode bit terdiri dari:

1. Cipher aliran
2. Cipher

DAFTAR PUSTAKA

Mrayati, M., Alam, Y. M. and At-Tayyan, H. 2002. 'Al Kindī's treatise on cryptanalysis. Series on Arabic Origins of Cryptology', *Damascus: KFCRIS & KACST*, 1.

Rinaldi. 2006. *Kriptografi*. Penerbit Informatika, Bandung.

Schneier. 1996. *Applied Cryptography, Second edition: Protocol, Algorithm and Source Code in C*. Wiley Computer Publishing, John Wiley & Sons, Inc.: NewYork. Available at: https://www.wiley.com/en-us/Applied+Cryptography:+Protocols,+Algorithms+and+Source+Code+in+C,+20th+Anniversary+Edition-p-9781119096726.

Wirdasari. 2008. 'Prinsip Kerja Kriptografi dalam Mengamankan Informasi', *SAINTIKOM*, 5 No. 2.

BAB 3
SYMMETERIC ENCRYPTION

Oleh Abdurrasyid

3.1 Pendahuluan

Penggunaan enkripsi dapat ditelusuri kembali ke zaman kuno, di mana ada kebutuhan akan komunikasi yang aman dan pribadi. Berikut adalah latar belakang singkat tentang mengapa dan bagaimana enkripsi muncul:

1. Enkripsi Kuno: Teknik enkripsi telah digunakan sejak zaman kuno untuk melindungi informasi sensitif. Contohnya termasuk sandi substitusi, di mana huruf atau simbol diganti dengan huruf atau simbol lain, dan sandi transposisi, di mana urutan huruf disusun ulang. Peradaban kuno seperti Mesir, Yunani, dan Roma menggunakan metode enkripsi untuk keperluan militer, diplomatik, dan komunikasi pribadi.
2. Penggunaan Militer dan Diplomatik: Enkripsi memainkan peran penting dalam urusan militer dan diplomatik sepanjang sejarah. Peradaban kuno, seperti Spartan, menggunakan perangkat enkripsi seperti scytale untuk mengirim pesan rahasia selama pertempuran. Enkripsi memungkinkan komandan militer dan diplomat untuk berkomunikasi dengan aman dan mencegah musuh mereka mencegat dan memahami pesan mereka.

   Perangkat enkripsi lainnya diproduksi dan digunakan selama periode waktu yang sama. "Mesin Besar" pemerintah AS terlihat seperti mesin tik awal tentang steroid. Mesin ini, secara resmi dikenal sebagai Sigaba, adalah satu-satunya mesin enkripsi yang kodenya tidak

dapat dipecahkan selama Perang Dunia II. Mesin lainnya adalah Typex, yang dirancang untuk komunikasi aman antara Inggris dan Amerika, mesin Tunney dan Sturgeon Amerika, yang mampu mengenkripsi dan mentransmisikan, dan mesin Purple dan Jade Jepang (Rhodes-Ousley, 2013).

3. Kemajuan dalam Kriptografi: Seiring waktu, kriptografi berkembang dengan kemajuan teknologi. Pada abad ke-20, mesin mekanis dan elektromekanis yang rumit, seperti mesin rotor Enigma, menyediakan metode enkripsi yang lebih canggih. Mesin ini digunakan oleh pemerintah dan organisasi militer untuk mengamankan komunikasi mereka.
4. Bangkitnya Enkripsi Berbasis Komputer: Dengan munculnya komputer, teknik enkripsi menjadi lebih maju dan dapat diakses secara luas. Pada tahun 1970-an, kriptografi kunci publik ditemukan, memungkinkan komunikasi yang aman melalui jaringan publik. Terobosan ini memungkinkan individu dan organisasi untuk mengenkripsi dan mendekripsi pesan menggunakan kunci publik dan pribadi.
5. Internet dan Enkripsi Modern: Meluasnya penggunaan internet dan kebutuhan akan transaksi online yang aman mengarah pada pengembangan standar enkripsi. Pengenalan *Advanced Encryption Standard* (AES) dan algoritme enkripsi lainnya memberikan kerangka kerja yang aman untuk melindungi data sensitif yang dikirimkan melalui internet.

Setiap teknologi enkripsi dari masa lalu masih digunakan sampai sekarang, dalam satu atau lain bentuk. Steganografi modern menyembunyikan pesan dalam file grafik web dan statis yang menyertai pesan radio. Anak-anak sekolah dan penulis jurnal

menyusun pesan menggunakan algoritme substitusi sederhana, dan one-time pad yang canggih direproduksi dalam token perangkat lunak dan perangkat keras. Demikian pula, stream cipher sering diproduksi dalam bentuk kode saat ini, contoh modernnya adalah RC4. Programmatic stream cipher menggunakan kunci untuk menghasilkan tabel kunci, dan kemudian satu byte dari tabel kunci dan satu byte teks biasa (teks yang tidak dienkripsi) di-XOR. Tabel kunci diremix dan byte baru dari tabel di-XOR-kan dengan byte berikutnya dari pesan teks biasa. Ketika seluruh pesan telah dienkripsi untuk menghasilkan ciphertext, baru data dikirim.

XOR, atau OR eksklusif, adalah pernyataan logika dimana satu dan nol dapat ditambahkan. Karena XOR bersifat reversibel, jika kunci asli dan algoritme untuk menghasilkan tabel diketahui, ciphertext dapat didekripsi. Sementara stream cipher bekerja pada satu karakter pada satu waktu, block cipher bekerja pada satu blok banyak bit dalam satu waktu. Fungsi Boolean nonlinear digunakan. Tidak seperti stream cipher, cipher blok awal tidak memvariasikan kunci, yang membuat hasilnya lebih mudah dipecahkan karena mengenkripsi kombinasi huruf yang sama menghasilkan ciphertext yang sama. Analisis frekuensi dapat digunakan secara efektif untuk memecahkan kode.

Cipher blok kemudian menggabungkan fungsi tambahan terhadap ciphertext untuk mengaburkan data yang berulang. DES, yang pernah menjadi standar enkripsi pemerintah AS, adalah cipher blok yang menggunakan 16 putaran aktivitas terhadap blok data 64-bit, dengan setiap putaran menambahkan lapisan kerumitan. Algoritma ini terkenal, tetapi tanpa kunci rahasia (yang panjangnya 40 atau 56 bit), sulit untuk mendekripsi. Faktanya, DES pernah dianggap sangat aman sehingga diperkirakan akan memakan waktu satu juta tahun sebelum dapat dipatahkan. Saat ini, sebagian besar komputer dapat merusak DES hanya dalam beberapa jam atau kurang. Ini adalah contoh perkiraan yang baik

berdasarkan daya komputasi pada titik waktu tertentu. Karena daya komputasi terus meningkat dan terus menjadi lebih murah, sesuai dengan hukum Moore, metode enkripsi demi metode enkripsi akan mudah dipecahkan.

Triple DES adalah peningkatan berikutnya untuk DES. Triple DES menggabungkan DES *ciphertext* dengan dirinya sendiri dan menggunakan hingga tiga kunci, sesuai dengan namanya. *Advance Encryption Standard*(AES) kini telah menggantikan DES dan Triple DES sebagai standar pemerintah federal AS yang baru. AES (yang sebenarnya adalah algoritma Rijndael) adalah algoritma cipher block yang menggunakan ukuran blok 128-bit, 192-bit, atau 256-bit dan ukuran kunci 128 bit.

Contoh lain dari block cipher adalah RC2 dan RC5 RSA, CAST milik Entrust, dan Blowfish Counterpane Systems. Tidak seperti DES, mereka dapat menggunakan kunci besar berukuran variabel. Untuk algoritme ini, ukuran kunci yang lebih besar menghasilkan enkripsi yang lebih kuat. Kriptografer akan terus merekomendasikan ukuran kunci yang terus meningkat untuk teknik enkripsi ini, karena daya komputasi mengejar kompleksitas algoritma.

National Institute of Standards and Technology AS (NIST) telah menerbitkan aturan tentang penggunaan enkripsi di dalam lembaga pemerintah AS, dalam Publikasi Khusus 800-131A. Sebagai pengakuan atas umur teknik enkripsi yang terbatas karena komputer tumbuh semakin kuat, publikasi ini menentukan tanggal akhir masa pakai untuk berbagai sistem kriptografi. Dalam publikasi ini, Triple DES memiliki dua panjang kunci, yang dikenal sebagai Triple DES dua kunci dan *Triple* DES tiga kunci. Triple DES dua kunci telah dinilai pada kekuatan keamanan 80 bit, sedangkan Triple DES tiga kunci dinilai pada kekuatan keamanan 112 bit. Skipjack, *sandi blok yang dikembangkan oleh* National Security Agency AS (NSA), dinilai dengan kekuatan keamanan 80 bit. AES memiliki tiga panjang kunci yang disetujui: 128, 192, dan 256 bit.

AES-128 dinilai dengan kekuatan keamanan 128 bit, AES 192 dengan kekuatan keamanan 192 bit, dan AES-256 dengan kekuatan keamanan 256 bit.

Tabel 3.1. Transisi Enkripsi Ditentukan dalam NIST SP800-131A, Menunjukkan Masa Hidup Terbatas untuk Sistem Kripto

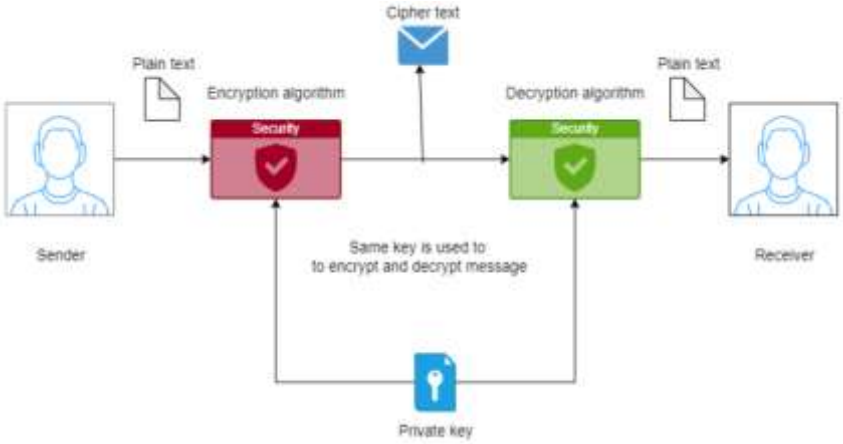
Algoritma	**Penggunaan**
Two - key Triple DES Encryption	• Dapat diterima hingga 2010 • Penggunaan terbatas dari 2011 hingga 2015 • Dilarang setelah 2015
Two - key Triple DES Decryption	• Dapat diterima hingga 2010 • Penggunaan tidak disarankan setelah 2010
Three - key Triple DES Encryption and Decryption	Saat ini dapat diterima
SKIPJACK Encryption	Dapat diterima hingga 2010
SKIPJACK Decryption	• Dapat diterima hingga 2010 • Penggunaan tidak disarankan setelah 2010
AES - 128 Encryption and Decryption	Saat ini dapat diterima
AES - 192 Encryption and Decryption	Saat ini dapat diterima
AES - 256 Encryption and Decryption	Saat ini dapat diterima

3.2 Pertukaran Kunci

Kriptografi adalah proses untuk mengubah teks biasa menjadi sandi menggunakan dua jenis kunci; kunci simetris dan asimetris. Simetris berarti bahwa kunci yang sama digunakan antara pengirim dan penerima dalam proses enkripsi dan dekripsi (Noor *et al.*, 2022).

Algoritme kriptografi simetris dasarnya menggunakan satu kunci rahasia. Kunci ini digunakan untuk mengenkripsi data, dan kunci yang sama, atau salinannya, digunakan untuk mendekripsi data. Kunci ini dapat digunakan untuk menghasilkan kunci lain, tetapi prinsipnya sama. Algoritma kunci tunggal dan simetris ini bekerja dengan baik selama kunci tersebut dapat dibagikan di antara pihak-pihak yang ingin menggunakannya. Di masa lalu, hal ini sering dilakukan dengan cara di luar batas, seperti menggunakan kurir atau kunjungan pribadi, atau cara lain yang tidak melibatkan komunikasi yang belum terjalin. Seiring waktu, kebutuhan kriptografi menyebar, dan dengan ini muncul kebutuhan yang meningkat untuk sering mengganti kunci untuk mencegah penemuan atau untuk mengurangi dampak dari kunci yang disusupi. Tidak selalu dimungkinkan bagi seseorang untuk bertemu, atau menskalakan metode di luar batas. Masalahnya menjadi jauh lebih sulit ketika Anda ingin menerapkan penggunaan kriptografi ke ribuan komunikasi yang dihasilkan oleh suatu mesin.
Cara untuk mengatasi masalah ini pertama kali diusulkan oleh Whitfield Diffie dan Martin Hellman. Protokol perjanjian kunci Diffie-Hellman menggunakan dua set kunci yang terkait secara matematis dan persamaan matematika kompleks yang memanfaatkan hubungan ini. Jika masing-masing dari dua komputer menghitung set kunci terkaitnya sendiri (tidak ada set yang terkait satu sama lain) dan berbagi salah satu kunci dengan komputer lain, mereka masing-masing dapat secara mandiri menghitung kunci rahasia ketiga yang akan sama di setiap komputer. Kunci rahasia ini dapat digunakan secara terpisah untuk

menghasilkan sejumlah kunci enkripsi simetris yang dapat digunakan oleh kedua komputer untuk mengenkripsi data yang berpindah dari satu komputer ke komputer lainnya. (Rhodes-Ousley, 2013).



Gambar 3.1. Cara kerja kunci kriptografi simetris(Noor *et al.*, 2022)

3.3 *Advanced Encryption Standard* (AES)

AES adalah cipher blok yang diadopsi sebagai standar untuk enkripsi simetris oleh *National Institute of Standard and Technology* (NIST) AS pada tahun 2001. AES adalah algoritma yang sangat aman dan tahan terhadap serangan. Ini juga sangat efisien, menjadikannya pilihan yang baik untuk aplikasi yang mengutamakan kecepatan dan efisiensi.

AES menggunakan kunci 128-bit, tetapi juga dapat menggunakan kunci 192-bit atau 256-bit. Semakin panjang kuncinya, semakin aman enkripsinya. Namun, kunci yang lebih panjang juga membutuhkan lebih banyak daya pemrosesan.

AES bekerja dengan cara membagi data yang akan dienkripsi menjadi blok-blok berukuran 128 bit. Blok kemudian

dienkripsi menggunakan serangkaian operasi matematika. Operasi spesifik yang digunakan dalam AES dirahasiakan, tetapi diketahui sangat kompleks.

Untuk mendekripsi data, kunci yang sama digunakan untuk melakukan operasi matematika yang sama secara terbalik. Ini membalikkan enkripsi dan membuat data dapat dibaca lagi. AES adalah algoritma yang sangat aman dan efisien yang banyak digunakan dalam berbagai aplikasi, antara lain:

1. Enkripsi data: AES digunakan untuk mengenkripsi data yang perlu dilindungi dari akses tidak sah. Ini termasuk data yang disimpan di disk, data yang dikirimkan melalui jaringan, dan data yang disimpan di cloud.
2. Enkripsi file: AES digunakan untuk mengenkripsi file yang perlu dilindungi dari akses tidak sah. Ini termasuk file yang berisi informasi sensitif, seperti kata sandi, nomor kartu kredit, dan nomor Jaminan Sosial.
3. Enkripsi komunikasi: AES digunakan untuk mengenkripsi komunikasi yang perlu dilindungi dari penyadapan. Ini termasuk komunikasi yang terjadi melalui jaringan, seperti email dan panggilan VoIP.

AES beroperasi pada blok data, biasanya 128 bit (16 byte) dalam satu waktu. Algoritma terdiri dari beberapa komponen kunci, antara lain ekspansi kunci, substitusi, permutasi, dan pencampuran kunci. Mari telusuri proses enkripsi AES selangkah demi selangkah menggunakan kunci 128-bit.

1. Ekspansi Kunci:
   Kunci asli diperluas untuk membuat satu set round key, satu untuk setiap putaran enkripsi. Round key diturunkan melalui serangkaian transformasi dan perhitungan. Untuk kunci 128-bit, dihasilkan 10 round key.

2. Putaran awal:
   A. AddRoundKey: Kunci putaran pertama di-XOR dengan blok plaintext (16 byte).

3. Putaran (1 sampai 9):
   Untuk setiap putaran:
   A. SubByte (Pergantian):
   Terapkan operasi SubBytes ke setiap byte matriks status menggunakan tabel pencarian S-box.

Kotak-S AES

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Tiap kolom ditentukan oleh nilai tempat satuan (nibel bawah) dan tiap baris ditentukan oleh nilai tempat enam belasan (nibel atas). Misalnya, $9a_{16}$ diubah ke $b8_{16}$.

Gambar 3.2. Kotak -S AES (Wikipedia, 2013)

B. ShiftRows (Permutasi):
Geser baris kedua satu posisi ke kiri.
Geser baris ketiga dua posisi ke kiri.
Geser baris keempat tiga posisi ke kiri.

C. MixColumns (Pencampuran):
Terapkan operasi MixColumns ke setiap kolom matriks status menggunakan perkalian matriks yang telah ditentukan sebelumnya.

D. AddRoundKey:
XOR matriks status dengan kunci bulat yang sesuai.

Putaran terakhir:
A. SubByte (Pergantian)
B. ShiftRows (Permutasi)
C. AddRoundKey

Matriks keadaan yang dihasilkan setelah putaran terakhir mewakili ciphertext.
Mari kita ilustrasikan proses enkripsi AES menggunakan contoh kasus:
Teks biasa: 00112233445566778899AABBCCDDEEFF
Kunci: 000102030405060708090A0B0C0D0E0F
Ekspansi Kunci:
Kunci asli diperluas untuk menghasilkan 11 round key (satu kunci awal dan 10 round key tambahan).
Putaran Awal:
AddRoundKey:
Teks biasa: 00112233445566778899AABBCCDDEEFF
Round Key: 000102030405060708090A0B0C0D0E0F
Hasil XOR: 00102030405060708090A0B0C0D0E0F0

Putaran (1 sampai 9):
Lakukan operasi berikut untuk setiap putaran:
A. SubByte:
Terapkan operasi SubBytes ke setiap byte matriks status menggunakan tabel pencarian S-box.

B. Pergeseran Baris:
Geser baris kedua satu posisi ke kiri.
Geser baris ketiga dua posisi ke kiri.
Geser baris keempat tiga posisi ke kiri.

C. Kolom Campuran:
Terapkan operasi MixColumns ke setiap kolom matriks status.

D. AddRoundKey:
XOR matriks status dengan kunci bulat yang sesuai.
Putaran terakhir:

Lakukan operasi berikut untuk putaran terakhir:
A. SubByte
B. PergeseranBaris
C. AddRoundKey

3.4 Kelebihan dan kekurangan enkripsi simetris

Keuntungan:

1. Cepat: Enkripsi simetris biasanya jauh lebih cepat daripada enkripsi asimetris (Tipton and Krause, 2008). Ini karena operasi matematis yang terlibat dalam enkripsi simetris kurang kompleks.
2. Sederhana: Enkripsi simetris relatif mudah diterapkan. Hal ini menjadikannya pilihan yang baik untuk aplikasi yang mengutamakan keamanan, dengan kompleksitas yang lebih mudah.

3. Efisien: Enkripsi simetris sangat efisien dalam hal kebutuhan bandwidth dan penyimpanan. Ini menjadikannya pilihan yang baik untuk aplikasi di mana data dalam jumlah besar perlu dienkripsi, Cocok untuk mengenkripsi file, disk, atau database..

Kekurangan:

1. Manajemen kunci: Kerugian utama dari enkripsi simetris adalah masalah manajemen kunci. Kunci rahasia harus dibagi antara pengirim dan penerima, dan ini bisa menjadi risiko keamanan. Kuncinya harus dirahasiakan, yang dapat menjadi tantangan ketika enkripsi dan dekripsi dilakukan di lokasi yang berbeda.
2. Kerentanan terhadap serangan:
    a. Enkripsi simetris rentan terhadap serangan jika kunci rahasia disusupi. Ini karena kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data.
    b. Kunci harus dikomunikasikan kepada pihak yang Anda bagikan datanya.
    c. Memerlukan metode pengiriman yang aman.
    d. Jika kuncinya disusupi, semua data yang dienkripsi dengan kunci itu juga disusupi.
    e. Tidak cocok untuk mengenkripsi data yang perlu dibagikan dengan banyak pihak.

Berikut beberapa pertimbangan tambahan saat menggunakan enkripsi simetris:

1. Panjang kunci: Semakin panjang kuncinya, semakin aman enkripsinya. Namun, kunci yang lebih panjang juga membutuhkan lebih banyak daya pemrosesan.
2. Algoritme: Algoritma yang berbeda memiliki kekuatan dan kelemahan yang berbeda. Beberapa algoritma lebih tahan terhadap serangan daripada yang lain.

3. Implementasi: Cara enkripsi simetris diterapkan juga dapat memengaruhi keamanannya. Algoritma yang diimplementasikan dengan baik lebih aman daripada algoritma yang diimplementasikan dengan buruk.

DAFTAR PUSTAKA

Noor, N. S. *et al.* 2022. 'A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication', *Computers*, 11(3). doi: 10.3390/computers11030039.

Rhodes-Ousley, M. 2013. *The Complete Information Security Second Edition*.

Tipton, H. F. and Krause, M. 2008. *Information security management handbook*, *Information Security Management Handbook, Sixth Edition*. doi: 10.1201/9781420067101.

Wikipedia. 2013. *Kotak-S Rijndael*, *Wikipedia*. Available at: https://id.wikipedia.org/wiki/Kotak-S_Rijndael.

BAB 4
ASYMMETRIC ENCRYPTION

Oleh Rima Rizqi Wijayanti

4.1 Pendahuluan

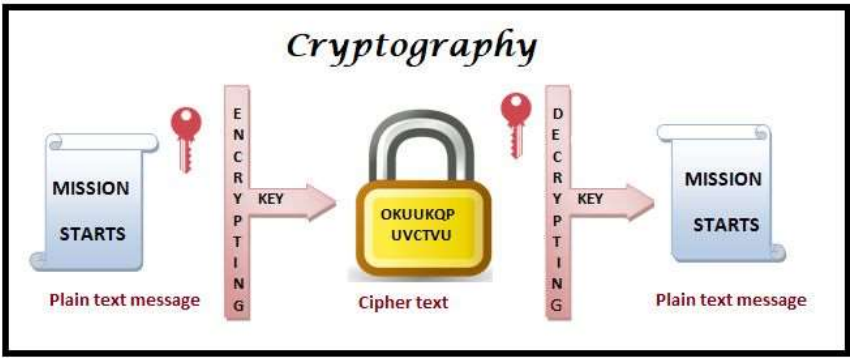
Jika pada bab sebelumnya dijelaskan mengenai enkripsi simetris, maka pada bab ini akan dijelaskan bagaimana jenis enkripsi asimetris.

Saat ini, enkripsi adalah komponen penting keamanan dunia maya, memastikan kerahasiaan dan integritas data di berbagai domain, termasuk perbankan online, e-niaga, dan platform komunikasi. Ini terus berkembang seiring munculnya ancaman dan teknologi baru, dengan upaya berkelanjutan untuk meningkatkan algoritma dan protokol enkripsi.

Enkripsi dapat digunakan untuk melindungi data bergerak maupun data statis dengan melindungi kerahasiaan data:

Untuk data yang bergerak, Anda dapat menerapkan protokol seperti IPSec untuk melindungi data yang sedang dikirim dari satu server ke server lainnya.

Untuk data saat yang tidak bergerak, Anda dapat mengimplementasikan alat seperti BitLocker pada sistem Microsoft Windows. Alat ini berfungsi untuk memastikan data di harddisk tetap terjaga kerahasiaannya jika harddisk dicuri(Tipton and Krause, 2008).



Gambar 4.1. Diagram alur alur kerja kriptografi (cyberhoot.com,2019)

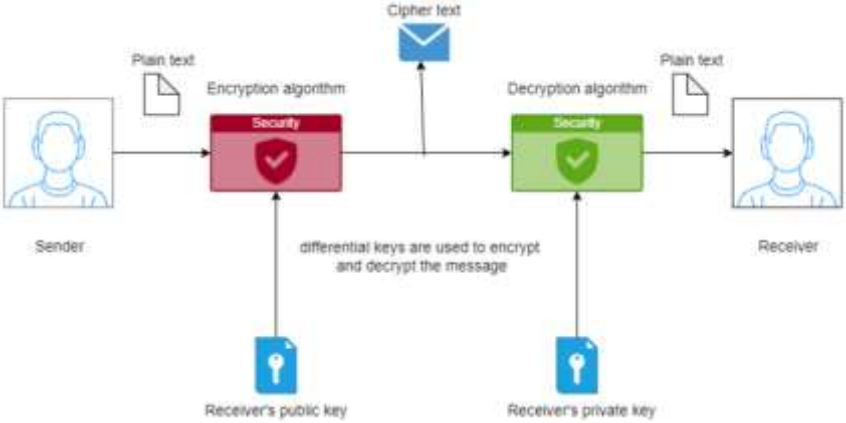
Bayangkan Anda memiliki pesan yang ingin Anda kirim dengan aman ke teman Anda. Tanpa enkripsi, siapapun yang menyadap pesan dapat dengan mudah membaca isinya. Namun, dengan menggunakan enkripsi, Anda dapat melindungi kerahasiaan pesan.

a. Proses Enkripsi:
   Anda mulai dengan pesan asli, yang dikenal sebagai teks biasa. Algoritma enkripsi mengambil teks biasa dan menerapkan transformasi matematis untuk mengubahnya menjadi bentuk alternatif yang disebut teks sandi(*ciphertext*). Ciphertext muncul sebagai kumpulan karakter yang tidak dapat dipahami tanpa kunci dekripsi.
b. Proses Dekripsi:
   Penerima, yang memiliki kunci dekripsi yang benar, menerapkannya pada ciphertext. Algoritma dekripsi membalikkan proses enkripsi, mengubah ciphertext kembali menjadi plaintext asli sehingga penerima dapat membaca pesan dalam bentuk aslinya.
   Enkripsi bergantung pada penggunaan kunci, yang pada dasarnya adalah sekumpulan instruksi atau parameter untuk algoritma enkripsi dan dekripsi. Kunci enkripsi digunakan

untuk mengubah plaintext menjadi ciphertext, sedangkan kunci dekripsi digunakan untuk membalikkan proses dan mengambil plaintext asli.

4.2 Asymmetric Encription

Kunci asimetris berarti terdapat dua kunci dalam proses enkripsi dan dekripsi, yaitu kunci privat dan kunci publik (Noor *et al.*, 2022).



Gambar 4.2. Cara kerja kunci kriptografi asymmetric(Noor *et al.*, 2022)

Untuk mengenkripsi pesan, pengirim menggunakan kunci publik penerima. Pesan terenkripsi hanya dapat didekripsi oleh penerima menggunakan kunci pribadi mereka. Ini karena kunci publik dan kunci privat terkait secara matematis, tetapi sedemikian rupa sehingga secara komputasi tidak mungkin untuk menurunkan kunci privat dari kunci publik.

Enkripsi asimetris sering digunakan untuk komunikasi yang aman melalui saluran yang tidak aman, seperti internet. Misalnya, saat Anda mengunjungi situs web yang menggunakan HTTPS, browser Anda mengenkripsi lalu lintas Anda menggunakan kunci publik situs web tersebut. Situs web kemudian mendekripsi lalu

lintas Anda menggunakan kunci pribadinya. Ini memastikan bahwa lalu lintas Anda tidak dapat dicegat dan dibaca oleh pihak ketiga.

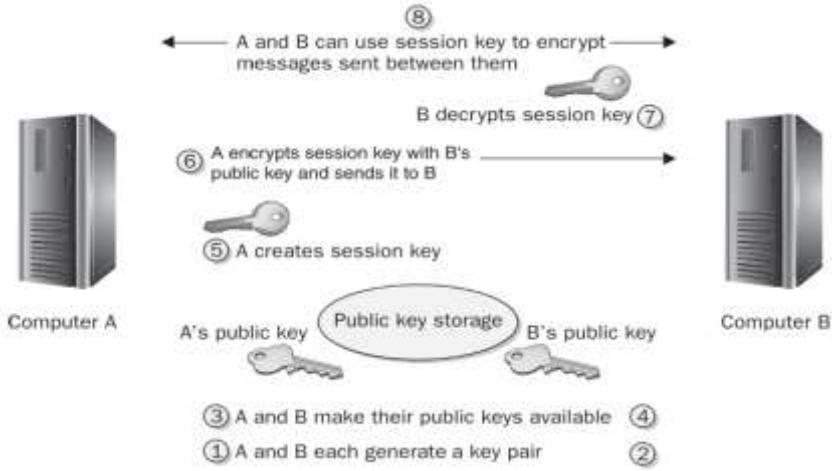
Enkripsi asimetris juga digunakan untuk tanda tangan digital. Tanda tangan digital adalah skema matematis untuk memverifikasi keaslian pesan atau dokumen digital. Ini biasanya digunakan untuk memverifikasi bahwa pesan belum dirusak sejak dikirim, dan bahwa pengirimnya adalah yang mereka klaim.

4.3 Enkripsi kunci publik

Enkripsi kunci publik adalah konsep pertama yang benar-benar revolusioner dalam kriptografi yang pertama kali diusulkan oleh Diffie dan Hellman. Enkripsi kunci publik, juga dikenal sebagai kriptografi kunci publik, adalah sistem kriptografi yang menggunakan sepasang kunci: kunci publik dan kunci pribadi. Kunci publik dapat dibagikan secara bebas di antara pengguna dan kunci privat, atau kunci rahasia, hanya diketahui oleh penerima. Kunci publik digunakan untuk mengenkripsi pesan atau konten dan kunci privat kemudian digunakan untuk mendekripsi pesan. Tujuan utama enkripsi kunci publik adalah untuk memberikan privasi, kerahasiaan, dan otentikasi. Algoritma kunci publik didasarkan pada fungsi matematika daripada operasi sederhana pada pola bit, seperti yang digunakan dalam algoritma enkripsi konvensional. Dalam sistem enkripsi kunci publik, ada enam bahan utama: plaintext, algoritma enkripsi, kunci publik, kunci privat, ciphertext, dan algoritma dekripsi.

Pasangan kunci publik/pribadi dapat digunakan untuk bertukar kunci sesi. Untuk melakukannya, setiap pihak yang perlu bertukar kunci menghasilkan sepasang kunci. Kunci publik dipertukarkan di antara para pihak atau disimpan dalam database. Kunci pribadi dirahasiakan. Jika diperlukan untuk bertukar kunci, satu pihak dapat mengenkripsinya menggunakan kunci publik pihak lain. Kunci terenkripsi kemudian ditransmisikan ke pihak lain. Karena hanya penerima yang dimaksud yang memegang kunci

privat yang terkait dengan kunci publik yang digunakan untuk mengenkripsi kunci sesi, hanya pihak tersebut yang dapat mendekripsi kunci sesi. Kerahasiaan kunci sesi terjamin, dan kemudian dapat digunakan untuk mengenkripsi komunikasi antara kedua pihak.



Gambar 4.3. Menggunakan kriptografi kunci publik untuk pertukaran kunci (Rhodes-Ousley, 2013).

4.4 Contoh penggunaan asymmetric encryption

Berikut adalah contoh bagaimana enkripsi asimetris dapat digunakan untuk mengirim pesan aman:

1. Raline menghasilkan kunci publik dan kunci privat.
2. Raline menerbitkan kunci publiknya di situs web publik.
3. Raffa ingin mengirimkan pesan aman kepada Raline. Dia menggunakan kunci publik Raline untuk mengenkripsi pesan.
4. Raline menerima pesan terenkripsi dan menggunakan kunci privatnya untuk mendekripsinya.

Hanya Raline yang dapat mendekripsi pesan tersebut karena hanya dia yang memiliki kunci privatnya. Ini memastikan bahwa pesan aman dan tidak dapat dibaca oleh orang lain.

Enkripsi asimetris adalah alat yang ampuh untuk mengamankan komunikasi dan data. Ini digunakan dalam berbagai aplikasi, termasuk email, enkripsi file, dan tanda tangan digital.

4.5 Infratruktur kunci publik

Infrastruktur Kunci Publik (PKI) telah menjadi salah satu bentuk enkripsi yang paling lazim dalam transaksi elektronik modern. Pasangan kunci terkait terikat dengan prinsip keamanan (pengguna atau komputer) dengan sertifikat. Sertifikat juga membuat kunci publik prinsip keamanan tersedia, sedangkan kunci privat terkait tetap disembunyikan. Otoritas sertifikat (CA) menerbitkan, membuat katalog, memperbarui, dan mencabut sertifikat di bawah pengelolaan kebijakan dan kontrol administratif. Tidak perlu membeli produk pihak ketiga untuk melakukannya, atau membeli sertifikat individual dari CA publik. (Namun, mungkin ada alasan tambahan untuk melakukannya, seperti untuk mendapatkan sertifikat SSL untuk situs e-niaga publik.) Versi Windows Server yang lebih baru terus menyediakan layanan CA dan menambahkan fungsionalitas. Misalnya, Windows Server 2003 Enterprise CA menawarkan templat sertifikat versi 2 dan Windows Server 2008 Enterprise CA menawarkan templat sertifikat versi 3 untuk memungkinkan kontrol dan penyesuaian lebih lanjut.

Beberapa CA dapat diatur dalam hierarki untuk keamanan, redundansi, dan keragaman geografis dan fungsional. CA dapat mengeluarkan berbagai jenis template. Pengguna atau komputer harus memiliki template yang dirancang dan disetujui untuk penggunaan tertentu agar dapat berpartisipasi dalam fungsi tertentu seperti mengenkripsi file atau menggunakan kartu pintar atau mendaftarkan pengguna lain.

CA yang terintegrasi dengan *Active Directory*, disebut Enterprise CA, menerbitkan berbagai jenis sertifikat, berdasarkan templat sertifikat bawaan. Pendaftaran dapat otomatis, manual dengan penerbitan otomatis, atau manual dan disetujui oleh Administrator CA. Izin yang ditetapkan pada templat selanjutnya menentukan kelompok pengguna dan komputer Windows mana yang benar-benar dapat memperoleh sertifikat. Windows Server 2003 memperkenalkan templat sertifikat versi 2, yang dapat disesuaikan dan menambahkan fitur seperti pendaftaran otomatis dan bahkan pengarsipan kunci. Pengarsipan kunci memungkinkan kunci pribadi yang terkait dengan sertifikat untuk disimpan di database pusat. Ini penting untuk pemulihan. File terenkripsi, misalnya, tidak dapat didekripsi tanpa kunci pribadi yang terkait dengan kunci publik yang digunakan untuk melindungi kunci enkripsi file. Dengan mengarsipkan kunci privat EFS, organisasi memastikan ketersediaan data, bahkan jika kunci asli dihancurkan atau rusak. Windows Server 2008 R2 memperkenalkan templat versi 3, yang menambahkan dukungan untuk Microsoft Crypto-API yang lebih baru, memberi administrator kemampuan untuk membuat sertifikat menggunakan penyedia layanan kriptografi (ECC) kriptografi kurva eliptik (ECC) yang lebih canggih dan aman.

4.6 Keuntungan dan Kelemahan penggunaan asymmetric encryption

Berikut adalah beberapa keuntungan dari enkripsi asimetris:

1. Enkripsi asimetris sangat aman. Secara komputasi tidak mungkin memecahkan enkripsi asimetris tanpa kunci privat.
2. Enkripsi asimetris serbaguna. Ini dapat digunakan untuk berbagai macam aplikasi, termasuk komunikasi yang aman, tanda tangan digital, dan pertukaran kunci.
3. Enkripsi asimetris dapat diskalakan. Ini dapat digunakan untuk mengamankan data dalam jumlah besar.

Berikut adalah beberapa kelemahan dari enkripsi asimetris:

1. Enkripsi asimetris lebih lambat dari enkripsi simetris. Ini karena operasi matematika yang terlibat dalam enkripsi asimetris lebih kompleks.
2. Enkripsi asimetris membutuhkan penggunaan dua kunci, yang bisa merepotkan.

4.7 Membuat enkripsi asimetrik sendiri

Ada beberapa cara untuk membuat kunci pribadi dan publik Anda sendiri. Berikut adalah beberapa metode:

1. Menggunakan baris perintah
   Jika Anda menggunakan sistem operasi mirip Unix, Anda dapat menggunakan perintah ssh-keygen untuk membuat pasangan kunci privat dan publik. Misalnya, untuk membuat pasangan kunci bernama id_rsa dan id_rsa.pub, Anda akan menjalankan perintah berikut:
   ssh-keygen -t rsa -b 2048 -f id_rsa
   Ini akan menghasilkan file kunci pribadi bernama id_rsa dan file kunci publik bernama id_rsa.pub di direktori saat ini.

2. Menggunakan alat grafis
   Ada juga sejumlah alat grafis yang dapat digunakan untuk menghasilkan kunci privat dan publik. Salah satu alat yang populer adalah PuTTYgen, yang tersedia untuk Windows, macOS, dan Linux.
   Untuk menghasilkan pasangan kunci privat dan publik menggunakan PuTTYgen, ikuti langkah-langkah berikut:
   a. Buka PuTTYgen.
   b. Klik pada tombol Generate.
   c. Gerakkan mouse Anda di sekitar layar untuk menghasilkan materi kunci acak.
   d. Masukkan frasa sandi untuk melindungi kunci pribadi Anda.

e. Klik tombol Save public key untuk menyimpan kunci publik.
f. Klik tombol Save private key untuk menyimpan kunci pribadi.

3. Menggunakan layanan online
   Ada juga sejumlah layanan online yang dapat digunakan untuk menghasilkan kunci privat dan publik. Salah satu layanan populer adalah Keygen.io. Untuk membuat pasangan kunci privat dan publik menggunakan Keygen.io, ikuti langkah-langkah berikut:
   a. Buka situs web Keygen.io.
   b. Klik pada tombol Generate.
   c. Masukkan frasa sandi untuk melindungi kunci pribadi Anda.
   d. Klik tombol Download untuk mengunduh kunci publik.
   e. Klik tombol Download untuk mengunduh kunci pribadi.
   f. Setelah Anda membuat kunci pribadi dan publik, Anda dapat menggunakannya untuk mengenkripsi dan mendekripsi data, atau untuk menandatangani dokumen digital.

4. Menggunakan open-ssl
   a. Unduh penginstal OpenSSL dari sumber tepercaya. Anda dapat mengunduh penginstal OpenSSL dari tautan unduhan resmi OpenSSL: https://slproweb.com/products/Win32OpenSSL.html
   b. Jalankan penginstal dan ikuti wizard penginstalan. Selama instalasi, pilih direktori untuk menginstal OpenSSL.
   c. Setelah instalasi, tambahkan direktori bin OpenSSL ke variabel lingkungan PATH sistem Anda. Ini akan

memungkinkan Anda untuk menjalankan perintah OpenSSL dari direktori mana pun di command prompt.

d. Untuk memverifikasi bahwa OpenSSL diinstal dengan benar, buka prompt perintah dan jalankan perintah **openssl version**. Ini akan menampilkan versi OpenSSL yang telah Anda instal.
e. Buka prompt perintah atau jendela terminal.
f. Arahkan ke direktori tempat Anda ingin menyimpan kunci.
g. Jalankan perintah berikut:
   openssl genrsa -out private_key.pem 2048
   Ini akan menghasilkan file kunci pribadi bernama private_key.pem dengan ukuran kunci 2048 bit.
h. Untuk mengekstrak kunci publik dari file kunci privat, jalankan perintah berikut:
   openssl rsa -in private_key.pem -outform PEM -pubout -out public_key.pem
   Ini akan menghasilkan file kunci publik bernama public_key.pem

Keterangan :

- genrsa - Ini adalah perintah untuk menghasilkan kunci pribadi.
- -out - Opsi ini menentukan nama file keluaran.
- 2048 - Ini adalah ukuran kunci dalam bit.
- -outform - Opsi ini menentukan format output.
- -pubout - Opsi ini mengekstrak kunci publik dari file kunci pribadi.

Secara keseluruhan, enkripsi asimetris adalah alat yang ampuh dan serbaguna untuk mengamankan komunikasi dan data. Ini digunakan dalam berbagai macam aplikasi, dan dianggap sangat aman. Namun, ini juga lebih lambat daripada enkripsi simetris, dan membutuhkan penggunaan dua kunci.

DAFTAR PUSTAKA

Noor, N. S. *et al.* 2022. 'A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication', *Computers*, 11(3). doi: 10.3390/computers11030039.

Rhodes-Ousley, M. 2013. *The Complete Information Security Second Edition*.

Tipton, H. F. and Krause, M. 2008. *Information security management handbook*, *Information Security Management Handbook, Sixth Edition*. doi: 10.1201/9781420067101.

BAB 5
STEGANALISIS

Oleh Marniyati H. Botutihe

5.1 Pendahuluan

Steganalisis merupakan teknologi yang bertujuan untuk menghadapi steganografi. Sasarannya adalah untuk menemukan keberadaan informasi rahasia bahkan merusak komunikasi yang bersifat rahasia. Steganalisis adalah teknologi penting dalam menyelesaikan masalah penggunaan steganografi secara kriminal. Peningkatan teknologi steganalisis membantu menghindari penggunaan steganografi yang melanggar hukum dan dapat berperan dalam mencegah kehilangan data pribadi, mengungkap data ilegal, melawan kekerasan, mencegah tragedi, serta memastikan keamanan publik dan stabilitas sosial. (Wu *et al.,* 2021).

Steganalisis dapat dimanfaatkan untuk mengetahui ada atau tidaknya pesan tersembunyi yang terkandung di dalam suatu media, dengan melihat adanya perubahan-perubahan ciri yang terjadi pada media tersebut. Steganalisis dapat dilakukan pada berbagai jenis media seperti teks, audio/suara, gambar, dan video (H. Liu, J. dkk, 2017). Sehebat apapun metode yang digunakan, jejak statistika penyisipan pasti akan tetap terekam. Sehingga, steganalisis pada umumnya dilakukan dengan cara membandingkan media yang menjadi suspect dengan media yang asli. Apabila ditemukan perbedaan diantara keduanya maka dapat ditarik kesimpulan bahwa mungkin terdapat pesan rahasia di dalamnya. Tahapan metode global dalam steganalisis adalah Membersihkan noise pada media (de-noising) DAN Mengekstraksi feature-feature yang ada (A. Madan and D. Gupta, 2014).

Tujuan steganalisis adalah mendeteksi data tersembunyi yang ditanamkan menggunakan teknik steganografi. Steganalisis melibatkan beberapa tugas yang berkaitan dengan data tersembunyi dalam media digital, seperti memprediksi muatan yang digunakan untuk menyisipkan data, memprediksi teknik steganografi yang digunakan, dan proses klasifikasi apakah file-file tersebut mengandung data tersembunyi atau tidak. Klasifikasi merupakan salah satu tugas yang paling penting dalam steganalisis. (Tabares-Soto, R.dkk, 2020)

Ada dua pendekatan dalam masalah steganalisis, yang pertama adalah menciptakan metode steganalisis yang khusus untuk algoritma steganografi tertentu. Yang kedua adalah mengembangkan teknik yang independen dari algoritma steganografi yang akan dianalisis. Setiap pendekatan memiliki kelebihan dan kekurangan sendiri. Teknik steganalisis yang khusus untuk metode penyisipan akan memberikan hasil yang sangat baik ketika diuji hanya pada metode penyisipan tersebut, namun mungkin gagal pada semua algoritma steganografi lainnya. Di sisi lain, metode steganalisis yang independen dari algoritma penyisipan mungkin memiliki tingkat akurasi yang lebih rendah secara keseluruhan, tetapi masih memberikan hasil yang dapat diterima pada algoritma penyisipan baru.

Pendekatan pertama yaitu Steganalisis yang dirancang dengan mempertimbangkan algoritma penyisipan steganografi tertentu. Algoritma steganografi dapat dibagi menjadi 3 kategori berdasarkan jenis gambar yang digunakan sebagai media penutup, yaitu gambar mentah (misalnya format bmp), gambar berbasis palet (misalnya gambar GIF), dan akhirnya gambar JPEG. Pendekatan kedua yaitu Teknik steganalisis yang dijelaskan di atas semuanya spesifik untuk suatu algoritma penyisipan tertentu, dirancang untuk bekerja dengan setiap algoritma penyisipan steganografi, bahkan algoritma yang tidak diketahui. Teknik-teknik seperti ini kemudian disebut sebagai teknik Universal Steganalysis

atau Teknik Blind Steganalysis. Teknik-teknik tersebut pada dasarnya merancang sebuah klasifikasi berdasarkan sekumpulan objek penutup (*cover-objects*) dan objek tersembunyi (*stego-objects*) yang diperoleh dari berbagai algoritma yang berbeda. (Kharrazi, Sencar and Memon, 2007)

5.2 Metode Steganalisis

Steganalisis adalah metode yang mendeteksi keberadaan data tersembunyi; proses ini dapat dikategorikan menjadi beberapa jenis seperti steganalisis statistik yang mencakup domain spasial, domain transformasi, dan steganalisis berbasis fitur. Steganalisis statistik membantu mendeteksi keberadaan pesan tersembunyi, analisis statistik dilakukan dengan piksel-piksel dan kemudian diklasifikasikan sebagai steganalisis domain spasial dan steganalisis domain transformasi. Pada domain spasial, pasangan piksel dianggap dan perbedaan antara mereka dihitung. Pasangan tersebut dapat berupa dua piksel tetangga apa pun. Mereka dapat dipilih dalam satu blok atau melintasi dua blok. Akhirnya, histogram digambarkan yang menunjukkan keberadaan pesan tersembunyi. Pada domain transformasi, hitungan frekuensi koefisien dihitung dan kemudian analisis histogram dilakukan saat steganalisis. Dengan bantuan ini, gambar sampul dan gambar stego dapat dibedakan. Namun, metode ini tidak memberikan informasi tentang algoritma penanaman data. Untuk mengatasi masalah ini, kita dapat memilih steganalisis berbasis fitur (L and B, 2017).

5.2.1 Analisis Statistik

Metode ini melibatkan analisis statistik terhadap media yang dicurigai mengandung pesan tersembunyi. Dalam analisis ini, distribusi statistik dari media yang sebenarnya dibandingkan dengan distribusi statistik dari media yang dicurigai mengandung pesan tersembunyi. Jika ada perbedaan signifikan antara distribusi statistik keduanya, dapat mengindikasikan keberadaan pesan tersembunyi.

5.2.2 Analisis Domain Spasial

Metode ini berfokus pada perubahan yang terjadi pada domain spasial (ruang piksel) media yang digunakan untuk menyembunyikan pesan. Ini melibatkan analisis terhadap piksel-piksel media yang dicurigai untuk mendeteksi pola, perubahan nilai piksel yang tidak biasa, atau perubahan dalam tekstur gambar.

5.2.3 Analisis Domain Frekuensi

Metode ini melibatkan analisis dalam domain frekuensi media yang dicurigai. Transformasi frekuensi seperti transformasi Fourier atau transformasi wavelet digunakan untuk mengidentifikasi perubahan dalam spektrum frekuensi yang dapat menunjukkan adanya pesan tersembunyi.

5.2.4 Analisis Redundansi

Metode ini memanfaatkan sifat redundansi dalam media komunikasi untuk mendeteksi pesan tersembunyi. Pesan tersembunyi seringkali memanfaatkan ruang yang tersedia di dalam media untuk disisipkan. Dengan menganalisis dan membandingkan struktur data media yang sebenarnya dengan media yang dicurigai, dapat ditemukan perbedaan yang menunjukkan adanya pesan tersembunyi.

5.2.5 Analisis Keseragaman

Metode ini memeriksa keseragaman atau konsistensi dari data yang disampaikan dalam media komunikasi. Jika ada pola atau perbedaan yang mencurigakan dalam data yang disampaikan, itu dapat menjadi indikasi adanya pesan tersembunyi.

5.2.6 Analisis Entropi

Metode ini melibatkan analisis entropi dari media yang dicurigai. Entropi digunakan untuk mengukur tingkat keacakan dalam data. Jika terdapat perubahan signifikan dalam entropi

media yang dicurigai, itu dapat menunjukkan adanya pesan tersembunyi.

5.2.7 Analisis Teknik Steganografi Yang Diketahui

Metode ini melibatkan pemahaman terhadap teknik steganografi yang umum digunakan. Dengan mempelajari algoritma dan metode steganografi yang diketahui, steganalisis dapat dilakukan dengan mencari tanda-tanda khas atau pola yang terkait dengan teknik tersebut.

5.3 Algoritma Steganalisis

Algoritma steganalisis dapat dikelompokkan menjadi dua berdasarkan metode steganografi yang ditargetkan, yaitu algoritma universal dan algoritma berbasiskan model. Metode steganalisis universal mencoba untuk memeriksa sejumlah metode steganografi, bahkan metode yang belum diketahui sekalipun, dalam framework yang umum. Algoritma steganalisis gambar digital berfokus pada ketergantungan antar piksel, yang merupakan dasar dari gambar-gambar alami. Sementara itu, algoritma steganalisis audio digital didasarkan pada aspek karakteristik file seperti ukuran distorsi sinyal audio dan statistik tingkat tinggi. Algoritma steganalisis untuk video digital menargetkan "kekurangan spasial dan temporal dalam sinyal video di dalam frame individu dan level antar frame". (Serrano, 2019)

5.4 Steganalisis Audio

Tujuan dari steganalisis audio adalah untuk mendeteksi perubahan apa pun dalam sinyal akibat penyisipan data. Terdapat dua domain utama untuk menyisipkan data, yaitu menggunakan domain spasial atau kadang-kadang menggunakan domain "waktu" atau "temporal", yang umumnya dilakukan dengan mengubah bit paling tidak signifikan (LSB) dari sampel data dalam file audio, atau dalam domain transformasi dengan memodifikasi parameter-

parameter yang berbeda dari sinyal. Selain itu, steganalisis audio diklasifikasikan berdasarkan format menjadi teknik steganalisis untuk format terkompresi seperti MP3 dan AAC, dan teknik steganalisis untuk format non-terkompresi. (Tabares-Soto, dkk, 2020)

5.5 Steganalisis Gambar

Sejarah steganalisis gambar dimulai pada akhir abad kedua puluh, dengan studi pertama yang diusulkan oleh Johnson dan Jajodia (Johnson, N.F, dkk, 1998.). Steganalisis gambar telah melalui perjalanan panjang mulai dari steganalisis visual dan ekstraksi fitur manual hingga penggunaan deep learning dan ekstraksi fitur otomatis. (Chandramouli, R, dkk, 2002).

5.6 Steganalisis Video

Kecepatan perkembangan internet telah menyebabkan penggunaan video yang luas. Video dapat diubah untuk mengirim pesan tersembunyi, oleh karena itu mendeteksi perubahan ini menjadi penting. Pada awalnya, teknik steganalisis untuk gambar langsung digunakan untuk mendeteksi perubahan yang dihasilkan dari pesan tersembunyi. Tetapi karena tidak banyak perubahan antara frame-frame berurutan dalam video, pendekatan-pendekatan ini tidak menghasilkan hasil yang baik. Oleh karena itu, terdapat perbedaan yang signifikan antara teknik steganalisis gambar dan teknik steganalisis video. Terdapat dua metode utama untuk mendeteksi pesan tersembunyi dalam video digital, yaitu metode berbasis vektor pergerakan dan metode berbasis tingkat antar-frame. Metode-metode ini telah digunakan dalam video dengan standar H.264/AVC dan, baru-baru ini, dalam standar HEVC. (Wang, P.; Cao, Y.; Zhao, X. 2017)

5.7 Steganalisis Tanda Tangan

Pada jenis ini, fitur-fitur dianggap sebagai pola atau tanda tangan unik. Oleh karena itu, jika teknik penyisipan steganografi diidentifikasi atau populer, menjadi mudah untuk memilih dan mengekstrak pola khusus yang sering muncul, seperti pengaturan histogram, rentang intensitas minimum dan maksimum, dan sebagainya. Jenis ini disebut sebagai tipe target atau spesifik, sementara yang lainnya adalah tipe universal di mana fitur-fitur diidentifikasi sebagai pola perilaku tanpa memandang teknik penyisipan. Beberapa teknik steganografi mengikuti akses berurutan atau linear dari unit media cover untuk penyisipan (AlSabhany, A.A., 2020).

5.8 Steganalisis Statistik

Steganalisis statistik terutama bergantung pada ekstraksi fitur statistik dan properti media cover dan stego. Ini juga mencakup metode target dan universal. Metode target dikembangkan dengan mempelajari dan menganalisis teknik penyisipan steganografi serta menentukan fitur statistik tertentu yang telah dimodifikasi akibat operasi penyisipan. Oleh karena itu, penting untuk memahami dengan baik teknik penyisipan untuk meningkatkan akurasi steganalisis. Hal ini akan menghasilkan kategori steganalisis lainnya tergantung pada domain penyisipan (Karampidis, K. dkk, 2018)

5.9 Steganalisis Mendalam

Kategori ini disebut steganalisis mendalam karena konsep fitur mendalam yang digunakan. Baru-baru ini, jaringan saraf menjadi tren dalam pembelajaran mendalam (*deep learning*) dan tugas klasifikasi karena akurasinya dan kemampuannya untuk memberikan pemahaman mendalam guna mencapai ketahanan dan efektivitas yang lebih tinggi dalam representasi semantik. Steganalisis mendalam mirip dengan steganalisis statistik universal

dalam hal tidak bergantung pada teknik steganografi penyisipan, namun perbedaannya adalah metode yang pertama mengekstrak fitur mendalam sementara yang terakhir mengekstrak fitur buatan tangan. Namun, metode ini masih baru dan memerlukan penelitian lebih lanjut (Dalal, M. dkk, 2020).

5.10 Jenis-jenis Steganalisis

Steganalisis dibagi menjadi dua bagian, yaitu Spesifik (*Targeted*) dan Generik (*Blind*). Berdasarkan ketergantungan pada Algoritma Steganografi (SA), steganalisis diklasifikasikan sebagai steganalisis terarah (*targeted*) dan steganalisis buta (*blind*).

Berdasarkan metode deteksinya, steganalisis juga dibagi berdasarkan alat deteksi, teknik pembelajaran mendalam (deep learning), serangan, dan metode penyisipan. Steganalis mencoba untuk menemukan pesan tersembunyi atau wilayah yang mencurigakan dengan melakukan serangan. Berikut ini adalah jenis-jenis steganalisis berdasarkan serangan: (Shamal Salunkhe, 2019)

5.10.1 Histogram Analysis

Analisis histogram digunakan untuk mengidentifikasi pola atau distribusi yang tidak biasa dalam histogram media yang dicurigai.

5.10.2 RS Analysis

Analisis *Redundancy and Symmetry* (RS) digunakan untuk mendeteksi pola redundansi atau simetri yang tidak wajar dalam media yang dicurigai.

5.10.3 Correlation Analysis

Analisis korelasi digunakan untuk mengidentifikasi pola korelasi yang tidak biasa antara piksel-piksel dalam media yang dicurigai.

5.10.4 Noise Analysis

Analisis kebisingan digunakan untuk mendeteksi penambahan atau modifikasi kebisingan yang tidak biasa dalam media yang dicurigai.

5.10.5 Visual Artifact Analysis

Analisis artefak visual digunakan untuk mengidentifikasi artefak atau distorsi visual yang tidak biasa dalam media yang dicurigai.

10.5.6 Compression Analysis

Analisis kompresi digunakan untuk membandingkan karakteristik kompresi media yang sebenarnya dengan media yang dicurigai, dan mencari perbedaan yang mencurigakan.

DAFTAR PUSTAKA

Wu, Z. et al. 2021. 'Steganography and steganalysis in voice over ip: A review', Sensors (Switzerland), 21(4), pp. 1–31. doi: 10.3390/s21041032.

H. Liu, J. Liu, R. Hu, X. Yan, and S. Wan, "Adaptive audio steganography scheme based on wavelet packet energy," in Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2017 IEEE 3rd International Conference on. IEEE, 2017, pp. 26–31.

A. Madan and D. Gupta, "Speech feature extraction and classification: A comparative review," International Journal of computer applications, vol. 90, no. 9, 2014.

Tabares-Soto, R.; Ramos-Pollán, R.; Isaza, G.; Orozco-Arias, S.; Ortíz, M.A.B.; Arteaga, H.B.A.; Rubio, A.M.; Grisales, J. A. A. 2020. Digital media steganalysis. In Digital Media Steganography.

Kharrazi, M., Sencar, H. T. and Memon, N. 2007. 'Image steganography and steganalysis: Concepts and practice', Mathematics And Computation In Imaging Science And Information Processing, (October), pp. 177–207. doi: 10.1142/9789812709066_0005.

L, R. and B, L. 2017. 'Approaches and Methods for Steganalysis – A Survey', Ijarcce, 6(6), pp. 433–438. doi: 10.17148/ijarcce.2017.6678.

Serrano, J. Steganalysis: A Study on the Effectiveness of Steganalysis Tools. Ph.D. Thesis, Utica College, Utica, NY, USA, 2019.

Chandramouli, R.; Li, G.; Memon, N.D. Adaptive steganography. In Security and Watermarking of Multimedia Contents IV; International Society for Optics and Photonics: Bellingham, WA, USA, 2002; Volume 4675, pp. 69–78.

Wang, P.; Cao, Y.; Zhao, X. Segmentation based video steganalysis to detect motion vector modification. Secur. Commun. Netw. 2017, 2017, 8051389.

AlSabhany, A.A.; Ali, A.H.; Ridzuan, F.; Azni, A.; Mokhtar, M.R. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Comput. Sci. Rev. 2020, 38, 100316.

Karampidis, K.; Kavallieratou, E.; Papadourakis, G. A review of image steganalysis techniques for digital forensics. J. Inf. Secur. Appl. 2018, 40, 217–235.

Dalal, M.; Juneja, M. Steganography and Steganalysis (in digital forensics): A Cybersecurity guide. Multimed. Tools Appl. 2020, 80, 5723–5771.

Salunkhe, S. and Bhosale, S. 2021. 'Feature extraction-based image steganalysis using deep learning', WEENTECH Proceedings in Energy, (February), pp. 188–198. doi: 10.32438/wpe.182021.

BAB 6
WATERMARKING

Oleh Irmawati

6.1 Pendahuluan

Bab ini membahas tentang konsep dasar watermaking, tujuan penggunaannya, dan pentingnya dalam konteks perlindungan konten digital. Watermarking adalah teknik yang digunakan untuk menyisipkan informasi tambahan ke dalam sebuah gambar, video, atau dokumen digital untuk tujuan identifikasi atau perlindungan. Pentingnya watermaking terletak pada perlindungan hak cipta, keaslian konten digital, dan melacak atau menelusuri konten yang telah disebarkan. Dalam era digital, dengan mudahnya reproduksi dan penyebaran konten secara online, perlindungan hak cipta dan keaslian konten menjadi semakin penting. Watermarking memberikan solusi untuk mengatasi tantangan ini dengan memberikan tanda pengenal yang unik pada setiap salinan konten digital (Mohanty and Florida, 1999).

Ada dua jenis watermarking yang umum digunakan:

1. Watermark yang terlihat (*Visible Watermarking*):
   Watermark yang terlihat secara jelas dan dapat dilihat oleh pengguna. Biasanya berupa teks atau logo yang disisipkan ke dalam gambar atau video. Tujuannya adalah untuk memberikan informasi tentang kepemilikan atau hak cipta, sehingga orang yang melihatnya dapat mengidentifikasi sumber asli dan menggunakan konten tersebut dengan izin yang tepat. Watermark terlihat juga dapat berfungsi sebagai penghambat untuk mencegah penggunaan yang tidak sah.

2. Watermark yang tidak terlihat (*Invisible Watermarking*): Watermark yang tidak terlihat oleh mata manusia secara langsung. Biasanya menggunakan algoritma dan teknik khusus untuk menyisipkan informasi tambahan ke dalam file digital. Watermark ini dapat dideteksi atau diekstraksi menggunakan alat atau perangkat lunak khusus. Tujuannya adalah untuk memberikan informasi yang sama seperti watermark terlihat, namun tanpa mengganggu estetika atau kualitas visual dari gambar atau video.

Proses watermarking melibatkan beberapa langkah, antara lain:

1. Pembuatan watermark: Membuat watermark yang sesuai dengan tujuan yang ingin dicapai, baik itu teks, logo, atau pola tertentu.
2. Sisipkan watermark: Menyisipkan watermark ke dalam gambar atau video menggunakan algoritma dan teknik tertentu. Watermark dapat ditempatkan di berbagai posisi di dalam konten digital, seperti pada sudut, tengah, atau sepanjang gambar.
3. Verifikasi dan validasi: Melakukan verifikasi untuk memastikan bahwa proses watermarking berhasil dan watermark terlihat atau tidak terlihat telah disisipkan dengan benar. Jika menggunakan watermark terlihat, perlu memastikan bahwa watermark tersebut mudah dibaca dan tidak mudah dihapus atau dimodifikasi.

Watermarking dapat digunakan dalam berbagai industri, seperti fotografi, periklanan, distribusi konten digital, dan perlindungan hak cipta. Meskipun watermarking dapat memberikan perlindungan tambahan, tetapi tidak sepenuhnya dapat mencegah pencurian konten. Namun, dengan menggunakan teknik yang canggih dan kombinasi metode watermarking yang

berbeda, dapat meningkatkan tingkat keamanan dan mengurangi risiko penyalahgunaan konten digital.

6.1.1 Pengantar Watermarking Digital

Watermarking digital adalah proses memasukkan informasi kecil dan tidak terlihat secara visual ke dalam suatu media digital, seperti gambar, video, atau audio, untuk tujuan autentikasi, keaslian, atau pelacakan (Cox *et al.*, 2002). Watermark digital biasanya tidak mengganggu kualitas atau konten media yang di watermark. Prinsip dasar dari watermarking digital adalah menyisipkan informasi tambahan ke dalam media digital yang tersembunyi dengan cara yang sulit dideteksi atau dihapus. Watermark dapat berupa teks, logo, gambar, atau kode unik lainnya yang ditanamkan ke dalam media digital. Informasi ini dapat digunakan untuk melacak atau melindungi hak cipta media, serta memverifikasi keaslian atau integritasnya.

Terdapat beberapa jenis watermarking digital, yaitu (Parashar and Singh, 2014):

1. Watermarking teks : melibatkan penambahan teks ke dalam media digital. Misalnya, dapat digunakan untuk menyisipkan informasi hak cipta atau nomor seri ke dalam gambar atau dokumen. Watermark teks biasanya tersembunyi secara visual, tetapi dapat dideteksi dan diekstrak dengan algoritma khusus.

   Proses Watermarking teks :

   a. Pemilihan teks : teks yang akan di watermark dipilih terlebih dahulu. Ini dapat berupa nama, logo, nomor seri, tanggal, atau informasi lain yang ingin disisipkan ke dalam media digital.
   b. Embedding : teks tersebut kemudian disisipkan ke dalam media digital dengan menggunakan algoritma watermarking untuk teks. Proses ini melibatkan pengubahan nilai-nilai piksel atau bit-bit media digital

secara cerdas sehingga teks tersembunyi tetapi sulit dideteksi atau dihapus.

c. Pendeteksian dan Ekstraksi : Saat media digital yang di-watermark dipindai atau dilihat, algoritma deteksi khusus digunakan untuk menemukan dan mengekstrak watermark teks dari media tersebut. Proses ini melibatkan analisis statistik atau teknik pengolahan sinyal untuk identifikasi watermark dan mengambil informasinya.

Contoh Kasus :

Salah satu contoh penggunaan watermarking teks adalah pada dokumen digital yang ingin dilindungi hak ciptanya. Seorang penulis atau penerbit dapat menyisipkan watermark teks yang berisi informasi hak cipta, seperti nama penulis, judul, atau tanggal penerbitan, ke dalam dokumen digital mereka. Watermark ini membantu dalam melacak atau membuktikan keaslian dokumen dan mencegah pencurian atau penyalahgunaan hak cipta.

2. Watermarking gambar : melibatkan penambahan elemen visual ke dalam gambar, seperti logo, untuk melindungi hak cipta atau memberikan informasi tambahan tentang gambar tersebut, tetapi dapat dideteksi oleh algoritma khusus.

   Proses Watermarking gambar :

   a. Pemilihan Watermark : watermark gambar dapat berupa logo perusahaan, nama fotografer, tanda hak cipta, atau elemen visual lainnya. Watermark ini haruslah terlihat jelas tetapi tidak mengganggu konten utama gambar.
   b. Embedding : watermark kemudian disisipkan ke dalam gambar dengan menggunakan teknik watermarking gambar. Proses ini melibatkan pengubahan piksel-piksel gambar secara cerdas sehingga watermark

tersembunyi namun sulit untuk dihapus tanpa merusak gambar asli.

c. Pendeteksian dan Ekstraksi : saat gambar yang di-watermark dipindai atau dilihat, algoritma deteksi khusus digunakan untuk mengidentifikasi dan mengekstrak watermark dari gambar. Proses ini melibatkan analisis warna, tekstur, atau fitur lainnya untuk mengungkap watermark yang tersembunyi.

Contoh Kasus :

Salah satu contoh penggunaan watermarking gambar adalah pada fotografi profesional yang ingin melindungi hak cipta dan mengidentifikasi gambar mereka. Seorang fotografer dapat menyisipkan watermark berupa logo atau nama mereka ke dalam sudut gambar menggunakan teknik watermarking gambar. Hal ini dapat membantu dalam melacak dan membuktikan keaslian gambar serta mencegah penggunaan tidak sah atau pencurian gambar tanpa izin.

3. Watermarking audio : biasanya digunakan dalam rekaman audio untuk menyisipkan informasi, seperti hak cipta, metadata, atau tanda penanda. Watermarking audio adalah proses menyisipkan informasi tersembunyi ke dalam sinyal audio digital dengan tujuan autentikasi, perlindungan hak cipta, atau melacak penggunaan tidak sah. Watermark audio biasanya berupa kode unik, metadata, atau tanda penanda yang disisipkan ke dalam sinyal audio tanpa mengganggu kualitas suara asli (Al-Haj, 2014).

   Proses Watermarking Audio :

   a. Pemilihan Watermark : watermark audio dapat berupa kode unik, informasi hak cipta, atau metadata lainnya yang ingin disisipkan ke dalam sinyal audio.

Watermark ini haruslah tersembunyi dan sulit dideteksi oleh pendengar manusia.

b. Embedding : watermark kemudian disisipkan ke dalam sinyal audio dengan teknik watermarking audio. Proses ini melibatkan pengubahan amplitudo, fase, atau spektrum frekuensi sinyal audio secara cerdas sehingga watermark tersembunyi namun dapat diidentifikasi dengan algoritma tertentu.
c. Pendeteksian dan Ekstraksi : saat sinyal audio yang di watermark diproses, algoritma deteksi khusus digunakan untuk mengenali dan mengekstrak watermark dari sinyal tersebut. Proses ini melibatkan analisis statistik, teknik pemrosesan sinyal, atau algoritma pembelajaran mesin untuk mengidentifikasi watermark dan mendapatkan informasinya.

Contoh Kasus :

a. Perlindungan Hak Cipta : produser musik atau label rekaman dapat menggunakan watermark audio untuk melindungi hak cipta lagu atau album mereka. Mereka dapat menyisipkan watermark berupa informasi hak cipta atau metadata ke dalam sinyal audio untuk melacak penggunaan yang tidak sah atau pencurian lagu.
b. Pelacakan Penggunaan Tidak Sah : watermark audio dapat digunakan untuk melacak penggunaan tidak sah atau penyebaran ilegal sinyal audio. Misalnya, stasiun radio dapat menyisipkan watermark yang unik ke dalam siaran mereka untuk melacak apakah siaran tersebut direkam dan disebarkan tanpa izin.
c. Identifikasi Asal-usul : dalam aplikasi forensik audio, watermark audio dapat digunakan untuk

mengidentifikasi asal-usul sinyal audio yang digunakan sebagai bukti dalam investigasi kriminal atau persidangan.

4. Watermarking video : melibatkan penambahan watermark ke dalam video untuk melacak atau melindungi hak cipta, atau memberikan informasi tambahan. Watermaking video biasanya adalah elemen visual seperti logo, teks, atau grafis yang disisipkan secara halus ke dalam bingkai video, dengan tetap menjaga kualitas visual secara keseluruhan (He, Yang and Zhu, 2012).

   Proses Watermarking video :

   a. Pemilihan watermarking : watermarking video berupa logo perusahaan, informasi hak cipta, atau elemen visual apa pun yang perlu disematkan ke dalam video. Watermarking harus terlihat tetapi tidak mengganggu konten video utama.
   b. Embedding : watermarking yang dipilih dimasukkan ke dalam bingkai video menggunakan teknik watermark video. Proses ini melibatkan modifikasi nilai piksel atau fitur video secara cerdas untuk menyembunyikan watermarking serta memastikan visibilitas dan ketahanannya terhadap penghapusan.
   c. Deteksi dan Ekstraksi : Saat video dengan watermark diproses, algoritma deteksi khusus digunakan untuk mengidentifikasi dan mengekstrak watermarking. Algoritma ini menganalisis bingkai video, seringkali menggunakan statistik atau teknik pemrosesan sinyal untuk mengungkap watermarking yang tersembunyi.

   Contoh Kasus Watermarking Video :

   a. Perlindungan Hak Cipta : watermark video digunakan oleh pemilik hak cipta untuk melindungi konten mereka dari penggunaan yang tidak sah. Misalnya, sebuah

perusahaan film dapat menyisipkan watermark berupa logo atau teks hak cipta mereka ke dalam video agar mudah mengidentifikasi jika ada penggunaan yang tidak diizinkan.

b. Pelacakan Penyebaran Ilegal : dalam kasus penyebaran video ilegal, watermark dapat digunakan untuk melacak asal-usul video yang diketahui sebagai sumber utama penyebaran ilegal. Dengan watermark yang unik, pemilik konten dapat mengidentifikasi penyebaran video yang tidak sah.
c. Identifikasi Brand : watermark video juga digunakan untuk tujuan branding. Misalnya, stasiun televisi sering menyisipkan watermark berupa logo mereka ke dalam siaran langsung atau acara untuk mempromosikan merek mereka kepada pemirsa.

6.1.2 Watermarking Dalam Keamanan Informasi

Watermarking dalam keamanan informasi merujuk pada proses menyisipkan informasi rahasia atau tanda khusus ke dalam data digital untuk melindungi integritas dan keaslian data tersebut. Tujuan utama dari watermarking adalah untuk memberikan identifikasi atau pelacakan, perlindungan hak cipta, atau deteksi pemalsuan terhadap data digital.

Watermarking dalam keamanan informasi digunakan dalam berbagai konteks, seperti :

1. Perlindungan hak cipta : Watermarking dapat digunakan untuk menandai data digital dengan hak cipta yang dimiliki oleh seseorang atau suatu organisasi. Hal ini membantu melacak penggunaan ilegal atau tidak sah dari data tersebut.
2. Verifikasi keaslian : Dengan menyisipkan watermark yang unik ke dalam data digital, dapat dilakukan verifikasi keaslian data tersebut. Misalnya, dalam fotografi atau

gambar medis, watermarking digunakan untuk memastikan bahwa gambar tersebut tidak mengalami perubahan atau pemalsuan.

3. Forensik digital : Watermarking dapat digunakan dalam analisis forensik untuk melacak sumber atau asal-usul data digital yang digunakan sebagai bukti dalam investigasi kriminal.
4. Pelacakan dan identifikasi : Watermarking dapat digunakan untuk memberikan tanda unik ke dalam data digital, sehingga dapat dilacak dan diidentifikasi jika data tersebut dicuri atau digunakan tanpa izin.

Watermarking merupakan salah satu metode yang penting dalam melindungi dan mengamankan data digital, terutama dalam era digital yang semakin berkembang pesat.

6.2 Dasar-Dasar Watermarking Digital

Teknologi watermarking digital adalah bidang baru dalam ilmu komputer, kriptografi, pemrosesan sinyal, dan komunikasi. Dasar-dasar watermarking digital melibatkan penambahan informasi rahasia ke dalam konten digital untuk tujuan perlindungan hak cipta, verifikasi keaslian, atau melacak sumber konten. Berikut adalah langkah-langkah dasar dalam proses watermarking digital:

1. *Embedding* (Penanaman): Pada tahap ini, watermark atau informasi rahasia disematkan ke dalam konten digital. Proses ini melibatkan teknik manipulasi data pada konten asli untuk menyisipkan informasi watermark. Watermark dapat berupa teks, logo, gambar, atau pola yang unik.
2. *Preprocessing* (Pra-Pemrosesan): Sebelum proses embedding, konten digital dapat melewati tahap pra-pemrosesan. Tujuannya adalah untuk mempersiapkan konten agar lebih cocok untuk penerapan watermark. Pra-

pemrosesan dapat meliputi teknik kompresi, normalisasi warna, atau penyesuaian kontras.

3. *Domain Selection* (Pemilihan Domain): Dalam tahap ini, dipilih domain atau ruang di mana watermark akan ditanamkan. Beberapa domain yang umum digunakan adalah domain spasial (piksel gambar), domain frekuensi (misalnya, transformasi Fourier), atau domain waktu (untuk audio atau video).
4. *Embedding Technique* (Teknik Penanaman): Pada tahap ini, digunakan teknik khusus untuk menyematkan watermark ke dalam konten digital. Teknik yang umum digunakan antara lain:
   a. *Least Significant Bit* (LSB): Teknik ini menggantikan bit terakhir dalam piksel gambar atau sampel audio dengan bit dari watermark.
   b. Transform Domain Techniques: Teknik ini melibatkan transformasi matematis pada konten digital (misalnya, Transformasi Fourier atau Transformasi Wavelet) untuk menyematkan watermark dalam domain frekuensi atau spasial.
   c. Spread Spectrum: Teknik ini menyematkan informasi watermark dengan cara menyebar dan menyembunyikannya di seluruh konten digital. Informasi tersebut kemudian dapat diekstraksi dengan kunci khusus.
5. *Extraction* (Ekstraksi): Pada tahap ini, watermark ditemukan atau diekstraksi dari konten digital yang sudah disisipi. Proses ekstraksi melibatkan teknik yang sesuai dengan teknik penanaman yang digunakan.

   Contoh sederhana dari watermarking digital adalah sebagai berikut:

   Misalkan Anda memiliki sebuah gambar dan ingin menyematkan watermark berupa logo pada sudut kanan

bawah gambar. Anda dapat menggunakan teknik *Least Significant Bit* (LSB) untuk melakukan ini. Setiap piksel di sudut kanan bawah gambar akan dimodifikasi dengan mengganti bit terakhir dengan bit dari logo tersebut. Ketika gambar tersebut ditampilkan, logo akan terlihat di sudut kanan bawah. Namun, proses ini tidak terlihat oleh mata manusia secara langsung.

Dalam praktiknya, metode watermarking digital yang lebih kompleks dan canggih digunakan untuk mencapai tujuan tertentu, seperti memberikan keaslian atau melindungi hak cipta.

6.3 Teknik Penanaman Watermark

Teknik penanaman watermark untuk menyisipkan watermark ke dalam data digital dengan cara yang tidak terdeteksi secara visual atau mengganggu data asli. Berikut ini adalah beberapa teknik penanaman watermark yang umum digunakan:

6.3.1 Watermarking di Domain Spasial

Teknik ini memanfaatkan karakteristik spasial dari data digital, seperti gambar. Watermark disisipkan dengan mengubah nilai piksel atau bit yang mewakili gambar. Contohnya, teknik yang umum digunakan adalah Least Significant Bit (LSB). Pada LSB, bit terakhir dari setiap piksel digunakan untuk menyimpan informasi watermark. Modifikasi ini biasanya tidak terlihat secara visual dan dapat diekstraksi dengan mudah.

Berikut adalah langkah-langkah umum yang terlibat dalam kasus watermarking di domain spasial:

1. Pilih gambar asli: Fotografer memilih gambar asli yang ingin dilindungi atau diidentifikasi.
2. Pilih watermark: Watermark dipilih berdasarkan preferensi atau kebutuhan fotografer. Ini bisa berupa teks, logo, atau kombinasi keduanya.

3. Proses penyisipan: Watermark disisipkan ke dalam gambar asli dengan teknik seperti Least Significant Bit (LSB) atau substitusi piksel. Pada teknik LSB, bit-bit watermark disimpan di bit terakhir dari piksel gambar. Proses ini dilakukan pada setiap piksel atau blok piksel, tergantung pada metode yang digunakan.
4. Verifikasi dan evaluasi: Setelah proses penyisipan, fotografer dapat memverifikasi keberadaan watermark dan menguji tingkat visibilitas atau ketahanannya terhadap serangan. Dalam beberapa kasus, perubahan visual mungkin tidak terlihat secara langsung, tetapi watermark masih dapat diekstraksi dengan tepat.
5. Watermark extraction: Untuk mengonfirmasi kepemilikan atau hak cipta, watermark dapat diekstraksi dari gambar yang telah diwatermarking. Proses ini melibatkan deteksi dan pemisahan watermark dari gambar asli.

6.3.2 Watermarking di Domain Frekuensi

Teknik ini melibatkan transformasi domain frekuensi dari data digital, seperti Transformasi Fourier atau Transformasi Wavelet. Transformasi ini mengubah data digital ke domain frekuensi, dimana komponen frekuensi yang lebih tinggi dapat dimanipulasi untuk menyimpan watermark. Setelah proses penyisipan, data digital dikembalikan ke domain spasial. Teknik ini lebih tahan terhadap serangan, tetapi memerlukan pemrosesan yang lebih kompleks.

Berikut adalah penjelasan dan contoh kasus watermarking berbasis domain frekuensi (Li and Lv, 2008):

1. Transformasi *Fourier Watermarking* : digunakan teknik ini untuk mengubah data digital ke domain frekuensi. Watermark disisipkan dengan memanipulasi koefisien frekuensi tertentu. Setelah proses penyisipan, data digital

dikembalikan ke domain spasial dengan menggunakan Transformasi Fourier invers.

Contoh kasus:

Misalkan seorang fotografer ingin melindungi hak ciptanya terhadap foto-foto yang diunggah ke situs web. Dia menggunakan watermarking berbasis Transformasi Fourier untuk menyisipkan tanda pengenal unik ke dalam gambar-gambar tersebut. Watermark disisipkan dengan mengubah koefisien frekuensi yang tinggi, yang tidak terlihat secara langsung pada gambar. Jika ada pengguna yang mencoba menghapus watermark atau mengedit foto, perubahan tersebut akan mempengaruhi koefisien frekuensi dan dapat terdeteksi saat proses ekstraksi watermark dilakukan.

2. Transformasi *Wavelet Watermarking* : menggunakan Transformasi Wavelet untuk mengubah data digital ke domain frekuensi. Transformasi Wavelet menghasilkan koefisien wavelet dengan tingkat resolusi dan frekuensi yang berbeda. Watermark disisipkan dengan memanipulasi koefisien wavelet yang sesuai. Setelah proses penyisipan, data digital dikembalikan ke domain spasial menggunakan Transformasi Wavelet invers.

   Contoh kasus:

   Dalam industri penyiaran, sebuah stasiun TV ingin menyisipkan watermark pada siaran televisi mereka untuk melacak konten yang tidak sah atau pelanggaran hak cipta. Mereka menggunakan teknik watermarking berbasis Transformasi Wavelet untuk menyisipkan tanda pengenal ke dalam video yang disiarkan. Watermark disisipkan pada koefisien wavelet yang lebih rendah, dimana perubahan tersebut minim terlihat secara visual. Saat video tersebut direkam atau disebarkan tanpa izin, watermark tetap ada dan dapat diekstraksi untuk mengidentifikasi sumber asli siaran.

6.3.3 Watermarking di Domain Transformasi

Watermarking jenis ini melibatkan penggunaan transformasi matematis pada data digital untuk menyisipkan watermark. Transformasi ini berupa transformasi Fourier, transformasi wavelet, atau transformasi lainnya. Teknik ini memanfaatkan representasi frekuensi atau domain lainnya dari data digital untuk menyembunyikan watermark (Fridrich, Goljan and Du, 2002).

1. Transformasi Fourier Watermarking:
   Pada teknik ini, data digital diubah ke dalam domain frekuensi menggunakan Transformasi Fourier. Komponen frekuensi yang tinggi dimanipulasi untuk menyisipkan watermark. Watermark disisipkan dengan mengubah nilai koefisien frekuensi tertentu pada domain Fourier. Setelah itu dikembalikan ke domain spasial dengan Transformasi Fourier invers.
2. Transformasi Wavelet Watermarking:
   Pada teknik ini, data digital diubah ke dalam domain wavelet menggunakan Transformasi Wavelet. Transformasi ini menghasilkan koefisien wavelet dengan tingkat resolusi dan frekuensi yang berbeda. Watermark disisipkan dengan memanipulasi koefisien wavelet yang sesuai. Setelah proses penyisipan, data digital dikembalikan ke domain spasial menggunakan Transformasi Wavelet invers.
   Contoh Kasus:
   Dalam industri sinema, seorang pembuat film ingin melindungi hak cipta terhadap film-film mereka yang diedarkan dalam format digital. Mereka menggunakan teknik watermarking berbasis Transformasi Wavelet untuk menyisipkan tanda pengenal ke dalam video. Watermark disisipkan pada koefisien wavelet yang lebih rendah, di mana perubahan tersebut minim terlihat secara visual

dalam video. Saat video tersebut direkam atau disebarkan tanpa izin, watermark tetap ada dan dapat diekstraksi untuk mengidentifikasi sumber asli film.

6.3.4 Watermarking di Domain Spectrum

Watermarking di Domain Spectrum adalah teknik yang digunakan untuk menyisipkan watermark ke dalam domain frekuensi sinyal audio atau gambar. Tujuan utama dari watermarking di domain spectrum adalah untuk melindungi keaslian dan integritas konten digital, serta memberikan perlindungan terhadap pencurian atau manipulasi yang tidak sah.

Proses watermarking di domain spectrum melibatkan transformasi Fourier dari sinyal asli ke domain frekuensi. Pada gambar, transformasi Fourier umumnya dilakukan dengan menggunakan Transformasi Fourier Cepat (*Fast Fourier Transform*/FFT). Sedangkan pada sinyal audio, transformasi Fourier sering kali menggunakan Transformasi Fourier Terkait (*Discrete Fourier Transform*/DFT) atau Variasi dari Transformasi Fourier Terkait, seperti Transformasi Fourier Terkait Cepat (*Fast Discrete Fourier Transform*/FFT).

Berikut adalah langkah-langkah umum yang terlibat dalam proses watermarking di domain spectrum:

1. Konversi ke domain frekuensi: sinyal asli (gambar atau audio) dikonversi ke domain frekuensi menggunakan teknik transformasi Fourier yang sesuai.
2. Penyisipan watermark: watermark, yang biasanya berupa pola atau sekumpulan bit, disisipkan ke dalam koefisien frekuensi yang dihasilkan dari transformasi Fourier. Koefisien frekuensi yang dipilih untuk penyisipan watermark harus dipilih secara hati-hati agar tidak mengganggu kualitas sinyal yang terlalu signifikan.
3. Inversi transformasi: setelah penyisipan watermark selesai, transformasi Fourier yang diubah dengan

watermark diinverskan untuk mengembalikan sinyal ke domain spasial atau waktu aslinya.

4. Deteksi watermark: saat sinyal yang disisipi watermark dikirim atau dipublikasikan, penerima atau pengguna dapat melakukan ekstraksi watermark menggunakan algoritme yang sesuai. Proses ekstraksi ini melibatkan transformasi Fourier lagi untuk mendapatkan koefisien frekuensi, dan kemudian dilakukan perbandingan dengan watermark asli untuk mendeteksi kehadiran watermark.

6.3.5 Watermarking Berbasis Kuantisasi

Watermarking berbasis kuantisasi adalah metode *watermarking* yang mengandalkan operasi kuantisasi untuk menyisipkan watermark ke dalam sinyal. Kuantisasi adalah proses pengurangan presisi atau representasi data ke dalam level yang lebih rendah, yang biasanya dilakukan dengan membagi rentang nilai menjadi level yang diskrit. Dalam konteks watermarking, kuantisasi digunakan untuk menyembunyikan informasi watermark ke dalam sinyal dengan mengubah beberapa nilai sampel.

Berikut adalah langkah-langkah umum yang terlibat dalam watermarking berbasis kuantisasi:

1. Penentuan watermark: watermark yang bisa berupa pola atau bitstream, ditentukan terlebih dahulu. Watermark ini biasanya berfungsi untuk mengidentifikasi atau melacak sumber atau pemilik konten.
2. Transformasi sinyal: sinyal asli (gambar atau audio) sering kali diubah ke dalam bentuk lain menggunakan transformasi seperti Transformasi Fourier Cepat (FFT) atau Transformasi Kosinus Diskret (DCT). Transformasi ini membantu dalam menggambarkan sinyal dengan basis yang lebih baik untuk operasi kuantisasi.

3. Kuantisasi: proses kuantisasi dilakukan pada koefisien transformasi yang dihasilkan dari langkah sebelumnya. Kuantisasi mengurangi presisi atau tingkat detail dengan memetakan nilai-nilai koefisien ke level-level yang diskrit. Beberapa nilai koefisien diganti dengan nilai baru sesuai dengan informasi watermark yang ingin disisipkan.
4. Inversi transformasi: setelah proses kuantisasi selesai, inversi transformasi dilakukan untuk mengembalikan sinyal ke domain aslinya.
5. Deteksi watermark: pada tahap ini, sinyal yang mengandung watermark dikirim atau dipublikasikan. Penerima atau pengguna dapat melakukan ekstraksi watermark dengan memproses sinyal menggunakan algoritme yang sesuai. Informasi watermark diekstraksi dengan membandingkan nilai-nilai koefisien kuantisasi dengan nilai-nilai watermark yang diharapkan.

Contoh aplikasi watermarking berbasis kuantisasi adalah perlindungan hak cipta pada gambar digital. Dalam konteks ini, informasi watermark seperti logo atau tanda identitas dapat disisipkan ke dalam koefisien kuantisasi gambar, yang kemudian dapat diekstraksi untuk membuktikan kepemilikan asli.

6.4 Teknik Ekstraksi dan Deteksi Watermark

Teknik ekstraksi dan deteksi watermark digunakan untuk mengidentifikasi dan mengambil watermark yang disisipkan dalam suatu media, seperti gambar atau video. Watermark adalah informasi tambahan yang disematkan ke dalam media sebagai tanda pengenal atau untuk tujuan keaslian, perlindungan hak cipta, atau pencatatan digital. Teknik ini dapat membantu dalam melacak dan melindungi keaslian media serta mencegah pelanggaran hak cipta.

6.4.1 Metode Ekstraksi Watermark

Metode ekstraksi watermark adalah teknik yang digunakan untuk mengambil watermark dari media yang telah disematkan padanya (Johnson, Duric and Jajodia, 2001). Ada beberapa metode yang umum digunakan untuk ekstraksi watermark, di antaranya:

1. Metode Korelasi: melibatkan perbandingan antara watermark yang diketahui dengan media yang diuji menggunakan operasi korelasi. Watermark diekstraksi dengan mencari korelasi tertinggi antara watermark dan media yang diuji. Metode korelasi dapat efektif jika watermark memiliki kekhususan yang tinggi dan tidak rentan terhadap serangan.
2. Metode Transformasi: melibatkan transformasi media ke domain transformasi seperti domain frekuensi (misalnya Transformasi Fourier atau Transformasi Gelombang Diskrit) atau domain spasial. Transformasi ini mengubah representasi media sehingga watermark dapat diidentifikasi dan diekstraksi dengan lebih mudah. Metode transformasi sering digunakan dalam konteks steganografi atau penyisipan informasi tersembunyi.
3. Metode Statistical: metode ini mengandalkan analisis statistik pada media untuk mengekstraksi watermark. Berbagai fitur statistik, seperti histogram atau distribusi probabilitas, dapat digunakan untuk mengidentifikasi keberadaan watermark. Metode ini dapat efektif dalam menghadapi serangan kecil atau modifikasi pada media.
4. Metode Pembelajaran Mesin: metode ini menggunakan algoritma pembelajaran mesin untuk mempelajari pola dan fitur dari media yang berisi watermark. Data latihan yang berisi contoh watermark yang diketahui digunakan untuk melatih model pembelajaran mesin. Setelah dilatih, model dapat digunakan untuk mengidentifikasi dan mengekstraksi watermark dari media yang tidak diketahui.

6.4.2 Deteksi dan Pemulihan Watermark

Deteksi dan pemulihan watermark adalah langkah-langkah dalam proses pengenalan watermark pada media yang telah disematkan watermark di dalamnya. Deteksi watermark melibatkan penggunaan teknik untuk mengidentifikasi keberadaan watermark dalam media yang diuji, sedangkan pemulihan watermark melibatkan proses mengembalikan atau mendapatkan kembali watermark yang mungkin telah mengalami kerusakan atau modifikasi.

Pemulihan watermark melibatkan usaha untuk memperoleh kembali atau memperbaiki watermark yang mungkin rusak atau termodifikasi pada media yang diuji. Beberapa metode yang digunakan dalam pemulihan watermark antara lain:

1. Restorasi Watermark:
   Metode ini bertujuan untuk mengembalikan watermark yang rusak atau termodifikasi pada media. Teknik restorasi, seperti pemulihan error koreksi atau teknik interpolasi, dapat digunakan untuk memperbaiki atau mengembalikan watermark yang rusak.
2. Rekonsiliasi Watermark:
   Pada kasus ketika media mengalami serangan atau modifikasi yang signifikan sehingga pemulihan watermark tidak memungkinkan, proses rekonsiliasi dapat dilakukan. Rekonsiliasi melibatkan penggunaan informasi yang masih tersedia dari watermark yang masih terdeteksi untuk memperoleh versi watermark yang lebih baik atau mendekati aslinya.

Proses deteksi dan pemulihan watermark seringkali merupakan bagian yang penting dalam sistem watermarking untuk memastikan keberhasilan pengenalan watermark dan integritasnya. Keefektifan teknik deteksi dan pemulihan tergantung pada kekuatan dan ketahanan watermark yang disematkan serta

kemampuan untuk mengatasi serangan atau modifikasi yang mungkin terjadi.

6.5 Ketahanan dan Keamanan Watermarking

Ketahanan dan keamanan watermarking adalah dua aspek penting dalam teknologi watermarking. Tujuan dari watermarking adalah untuk melindungi keaslian dan integritas data, serta untuk melacak dan mencegah penggunaan yang tidak sah atau pemalsuan.

Ketahanan watermarking merujuk pada kemampuan suatu watermark untuk tetap bertahan atau terdeteksi setelah data yang memuat watermark tersebut mengalami serangan. Transformasi atau serangan tersebut dapat berupa kompresi, cropping, filterisasi, atau manipulasi lainnya. Dalam konteks ini, ketahanan watermarking berkaitan dengan kemampuan suatu sistem watermarking untuk mempertahankan watermarknya yang tersembunyi dan dapat terdeteksi bahkan setelah pemrosesan atau serangan terhadap data.

Keamanan watermarking, di sisi lain, berkaitan dengan kerahasiaan dan keamanan informasi yang disisipkan dalam watermark. Ini terutama relevan ketika informasi yang disisipkan dalam watermark adalah rahasia atau memiliki nilai penting yang perlu dilindungi dari pihak yang tidak berwenang. Keamanan watermarking melibatkan penggunaan teknik kriptografi dan metode pengacakan untuk melindungi informasi watermark dari akses yang tidak sah atau pemalsuan oleh pihak yang tidak berwenang.

Watermarking digunakan dalam bidang forensik digital untuk menganalisis keaslian dan integritas bukti digital dalam investigasi kriminal atau perdata.

6.5.1 Keamanan Watermark terhadap Serangan Jahat

Keamanan watermark terhadap serangan jahat adalah aspek penting dalam teknologi watermarking yang bertujuan

untuk melindungi informasi yang disisipkan dalam watermark dari akses yang tidak sah atau pemalsuan oleh pihak yang tidak berwenang. Serangan jahat dalam konteks ini mencakup berbagai upaya yang dilakukan oleh pihak yang tidak berwenang untuk menghilangkan, memodifikasi, atau memalsukan watermark, atau bahkan mencuri informasi yang terkandung dalam watermark.
Serangan jahat yang mungkin terjadi dalam kasus ini meliputi:

1. Penghilangan Watermark: pihak yang tidak berwenang dapat mencoba menghilangkan watermark dari salinan film untuk menghindari pelacakan atau pendeteksian. Mereka dapat menggunakan teknik penghapusan atau penyisipan noise untuk mengaburkan atau menghapus informasi watermark yang ada.
2. Modifikasi Watermark: pihak yang tidak berwenang mungkin mencoba memodifikasi informasi yang terkandung dalam watermark untuk memalsukan identitas salinan film atau mengubah informasi hak cipta yang terkait. Mereka dapat melakukan perubahan pada bit watermark yang ada atau menyisipkan watermark palsu.
3. Pencurian Informasi Watermark: pihak yang tidak berwenang dapat mencoba mencuri informasi rahasia atau kunci yang terkandung dalam watermark untuk melakukan pemalsuan atau penggunaan yang tidak sah. Mereka dapat menggunakan teknik analisis atau serangan kriptografi untuk mengungkapkan atau mencuri informasi watermark yang terenkripsi.

Untuk melawan serangan-serangan jahat tersebut, teknik-teknik berikut dapat digunakan dalam keamanan watermark:

1. Kriptografi: mengenkripsi informasi watermark sebelum disisipkan dalam data atau menggunakan teknik kriptografi untuk melindungi informasi kunci yang terkandung dalam watermark. Ini akan mempersulit pihak

yang tidak berwenang untuk mencuri atau memodifikasi informasi watermark.

2. Pengacakan: menggunakan metode pengacakan untuk mengacak posisi atau urutan bit dalam watermark. Ini akan mengurangi kemungkinan serangan yang berhasil karena pihak yang tidak berwenang tidak dapat dengan mudah memahami atau memprediksi struktur watermark yang telah diacak.
3. Deteksi dan Rekonsiliasi: menambahkan mekanisme deteksi untuk mendeteksi serangan atau modifikasi terhadap watermark. Misalnya, menggunakan metode checksum atau pengkodean untuk memeriksa integritas watermark setelah pengolahan atau serangan. Jika terdeteksi adanya perubahan atau penyisipan yang tidak sah, tindakan yang tepat dapat diambil untuk mengatasi serangan tersebut.

6.6 Aplikasi Watermarking

Aplikasi watermarking adalah perangkat lunak yang dirancang khusus untuk menambahkan watermark ke dalam konten digital, seperti gambar, video, atau dokumen. Aplikasi ini menyediakan berbagai fitur dan pengaturan yang memungkinkan pengguna untuk menyesuaikan tampilan, ukuran, transparansi, dan posisi watermark sesuai dengan kebutuhan mereka. Berikut ini adalah penjelasan mengenai aplikasi watermarking:

1. Fungsi dan Tujuan:
2. Aplikasi watermarking bertujuan untuk melindungi konten digital dari pencurian atau penggunaan yang tidak sah. Dengan menambahkan watermark, pemilik konten dapat memperoleh pengakuan sebagai pemilik yang sah dan melacak asal-usul konten tersebut.
3. Watermark juga dapat digunakan untuk branding dan promosi. Dengan menampilkan logo atau nama perusahaan

pada konten, aplikasi watermarking membantu dalam memperkenalkan merek dan membangun kesadaran merek.

4. Fitur dan Pengaturan:
    a. Tampilan Watermark: Aplikasi ini memungkinkan pengguna untuk memilih jenis watermark yang ingin ditambahkan, seperti teks, logo, atau gambar khusus. Pengguna juga dapat menyesuaikan tampilan watermark, seperti font, warna, ukuran, dan efek visual seperti transparansi atau bayangan.
    b. Posisi dan Penempatan: Aplikasi watermarking menyediakan pengaturan untuk menentukan posisi watermark pada konten. Pengguna dapat memilih untuk menempatkannya di pojok, tengah, atau di lokasi khusus pada gambar atau video.
    c. Transparansi dan Opacity: Pengguna dapat mengatur tingkat transparansi atau kecerahan watermark. Ini memungkinkan watermark tetap terlihat tanpa mengganggu konten asli secara berlebihan.
    d. Batch Watermarking: Beberapa aplikasi mendukung penambahan watermark dalam jumlah besar secara otomatis. Ini memudahkan pengguna untuk menambahkan watermark ke sejumlah file sekaligus, menghemat waktu dan usaha.
5. Penggunaan pada Jenis Konten Tertentu:
    a. Gambar: Aplikasi watermarking untuk gambar memungkinkan pengguna untuk menambahkan watermark ke foto-foto mereka. Pengguna dapat memilih untuk menampilkan teks, logo, atau gambar transparan pada sudut gambar atau di sepanjang bidang utama.
    b. Video: Aplikasi watermarking untuk video memungkinkan pengguna untuk menambahkan

watermark ke dalam video mereka. Watermark dapat ditampilkan dalam bentuk overlay tetap atau bergerak di sepanjang durasi video.

c. Dokumen: Dalam hal dokumen, aplikasi watermarking dapat digunakan untuk menambahkan watermark teks ke halaman-halaman dokumen. Misalnya, pemilik dokumen dapat menambahkan "Draf" atau "Hak Cipta" pada dokumen untuk mengidentifikasinya.

6. Aplikasi Watermarking Populer:
   a. Adobe Photoshop: Photoshop adalah perangkat lunak pengeditan gambar yang juga menyediakan fitur untuk menambahkan watermark pada gambar.
   b. CorelDRAW: CorelDRAW adalah aplikasi desain grafis yang mencakup fitur watermarking untuk gambar dan dokumen.

DAFTAR PUSTAKA

Al-Haj, A. 2014. 'An imperceptible and robust audio watermarking algorithm', *EURASIP Journal on Audio, Speech, and Music Processing*, 2014(1), pp. 1–12.

Cox, I. *et al.* 2002. 'Digital watermarking', *Journal of Electronic Imaging*, 11(3), p. 414.

Fridrich, J., Goljan, M. and Du, R. 2002. 'Lossless data embedding for all image formats', in *Security and watermarking of multimedia contents IV*. SPIE, pp. 572–583.

He, Y., Yang, G. and Zhu, N. 2012. 'A real-time dual watermarking algorithm of H. 264/AVC video stream for Video-on-Demand service', *AEU-International Journal of Electronics and Communications*, 66(4), pp. 305–312.

Johnson, N.F., Duric, Z. and Jajodia, S. 2001. *Information hiding: steganography and watermarking-attacks and countermeasures: steganography and watermarking: attacks and countermeasures*. Springer Science & Business Media.

Li, B. and Lv, H. 2008. 'Image watermarking based on dual tree complex wavelet transform and pulse coupled neural network', in *2008 Fourth International Conference on Natural Computation*. IEEE, pp. 578–582.

Mohanty, S.P. and Florida, S. 1999. 'Digital Watermarking : A Tutorial Review', *Channels* [Preprint].

Parashar, P. and Singh, R.K. 2014. 'A survey: digital image watermarking techniques', *International Journal of signal processing, image processing and pattern recognition*, 7(6), pp. 111–124.

BAB 7
WIRELESS SECURITY

Oleh Iwan Adhicandra

7.1 Pendahuluan

7.1.1 Definisi Wireless Security

Keamanan nirkabel atau *Wireless Security* merujuk pada langkah-langkah yang dirancang untuk melindungi sistem dan jaringan nirkabel dari ancaman dan serangan. Ini mencakup berbagai metode keamanan yang digunakan untuk mencegah akses yang tidak sah, mencuri data, merusak perangkat, atau melakukan aktivitas jahat lainnya melalui sistem atau jaringan nirkabel. Keamanan ini bisa diterapkan pada berbagai sistem nirkabel termasuk jaringan Wi-Fi, perangkat seluler seperti smartphone dan tablet, serta perangkat IoT (*Internet of Things*) lainnya.

7.1.2 Sejarah dan Perkembangan Wireless Security

Wireless security mulai menjadi perhatian seiring dengan perkembangan dan penyebaran teknologi nirkabel. Sejak kemunculan Wi-Fi pertama pada tahun 1997, telah ada banyak perubahan dalam teknologi dan standar keamanan. Protokol keamanan awal seperti WEP (*Wired Equivalent Privacy*) yang awalnya dirancang untuk memberikan tingkat keamanan yang sama dengan jaringan kabel, segera ditemukan memiliki sejumlah kelemahan serius.

Ini memicu pengembangan protokol keamanan yang lebih baik seperti WPA (*Wi-Fi Protected Access*), dan versi berikutnya seperti WPA2 dan WPA3. Selain itu, peningkatan ancaman dan serangan cyber juga telah mendorong inovasi dalam teknologi dan

praktek terbaik keamanan nirkabel, seperti penggunaan firewall, VPNs, dan sistem pencegahan intrusi.

7.1.3 Pentingnya Wireless Security

Keamanan nirkabel sangat penting dalam dunia digital saat ini. Dengan semakin banyaknya perangkat yang terhubung secara nirkabel, jaringan dan data yang dikendalikan melalui perangkat ini menjadi sasaran yang menarik bagi para pelaku cyber. Tanpa pengamanan yang tepat, data sensitif bisa dicuri, perangkat bisa diambil alih, dan jaringan bisa dilumpuhkan.

Selain itu, banyak peraturan dan standar, seperti GDPR (*General Data Protection Regulation*) Uni Eropa dan *California Consumer Privacy Act* (CCPA), sekarang mengharuskan organisasi untuk melindungi data pelanggan mereka, termasuk data yang dikirim dan diterima melalui jaringan nirkabel. Melanggar peraturan ini bisa mengakibatkan denda besar dan kerusakan reputasi.

Dengan kata lain, keamanan nirkabel tidak hanya penting untuk menjaga operasional sehari-hari suatu organisasi, tetapi juga penting untuk mematuhi hukum dan menjaga kepercayaan pelanggan.

7.2 Dasar-Dasar Wireless Security

7.2.1 Cara Kerja Wireless Networks

Jaringan nirkabel atau *wireless networks* bekerja dengan menggunakan gelombang radio atau inframerah untuk mengirim dan menerima data. Pada jaringan Wi-Fi, misalnya, perangkat keras yang disebut router atau access point mengirimkan sinyal yang dapat diterima oleh perangkat lain yang dilengkapi dengan kartu jaringan nirkabel. Data kemudian dikirim dan diterima melalui sinyal ini. Faktor yang mempengaruhi kualitas sinyal dan jangkauan jaringan antara lain adalah frekuensi gelombang yang digunakan, hambatan fisik, dan kondisi lingkungan.

7.2.2 Risiko dan Ancaman Keamanan dalam Wireless Networks

Ada berbagai risiko dan ancaman keamanan yang berpotensi mengganggu atau merusak jaringan nirkabel. Beberapa ancaman utama meliputi:

Eavesdropping: Pelaku dapat "mendengarkan" atau mencegat transmisi data yang dikirim melalui jaringan nirkabel, kemungkinan mengakses informasi yang sensitif.

Unauthorized Access: Jika jaringan tidak diproteksi dengan baik, pengguna yang tidak berwenang bisa mendapatkan akses, menggunakan sumber daya jaringan, atau merusak sistem.

Man-In-The-Middle Attacks: Dalam serangan jenis ini, pelaku menempatkan diri mereka di antara dua pihak yang berkomunikasi, memungkinkan mereka untuk mencegat dan memanipulasi data.

Denial of Service Attacks: Serangan ini dilakukan dengan membanjiri jaringan dengan lalu lintas yang tidak perlu, sehingga jaringan menjadi tidak responsif atau lambat.

7.2.3 Prinsip-prinsip Keamanan Wireless

Prinsip-prinsip keamanan wireless utama mencakup:

Autentikasi: Ini melibatkan verifikasi identitas pengguna atau perangkat sebelum memberikan akses ke jaringan. Autentikasi bisa dilakukan melalui metode seperti password, sertifikat digital, atau otentikasi dua faktor.

Enkripsi: Ini melibatkan penggunaan algoritma untuk mengubah data menjadi format yang tidak bisa dibaca tanpa kunci dekripsi yang tepat. Enkripsi membantu melindungi data dari mata-mata atau pelaku yang mungkin mencegat transmisi.

Integritas: Ini berkaitan dengan menjaga keakuratan dan konsistensi data. Langkah-langkah harus diambil untuk mencegah data diubah atau rusak selama transmisi.

Access Control: Ini melibatkan pengaturan hak akses untuk pengguna dan perangkat dalam jaringan. Pengguna dan perangkat harus diberi akses minimum yang mereka butuhkan untuk melakukan tugas mereka, prinsip ini sering disebut dengan istilah "*least privilege*".
Availability: Ini berkaitan dengan memastikan bahwa jaringan dan data selalu tersedia untuk pengguna yang berwenang. Ini bisa melibatkan langkah-langkah seperti menjaga perangkat keras dan perangkat lunak jaringan tetap up to date dan melindungi terhadap serangan denial

7.3 Protokol Keamanan Wireless

7.3.1 *Wired Equivalent Privacy* (WEP)

WEP adalah protokol keamanan nirkabel yang pertama kali diperkenalkan sebagai bagian dari standar Wi-Fi 802.11 pada tahun 1997. Tujuan dari WEP adalah untuk memberikan tingkat keamanan yang setara dengan jaringan kabel. Namun, WEP memiliki banyak kelemahan keamanan dan bisa dipecahkan dengan relatif mudah, sehingga sekarang jarang digunakan.

7.3.2 *Wi-Fi Protected Access* (WPA)

WPA diperkenalkan pada tahun 2003 sebagai pengganti sementara untuk WEP, dan menawarkan peningkatan keamanan yang signifikan. WPA menggunakan teknik enkripsi yang disebut TKIP (*Temporal Key Integrity Protocol*), yang secara dinamis mengubah kunci enkripsi setelah setiap paket data, membuatnya jauh lebih sulit untuk ditembus.

7.3.3 *Wi-Fi Protected Access* II (WPA2)

WPA2, yang diperkenalkan pada tahun 2004, adalah peningkatan dari WPA dan sekarang menjadi standar keamanan nirkabel yang paling banyak digunakan. WPA2 menggantikan TKIP dengan AES (*Advanced Encryption Standard*), sebuah standar

enkripsi yang jauh lebih kuat. WPA2 juga mendukung autentikasi jaringan menggunakan protokol yang disebut 802.1X, yang sangat berguna dalam pengaturan bisnis dan perusahaan.

7.3.4 *Wi-Fi Protected Access* III (WPA3)

WPA3 adalah versi terbaru dari protokol WPA dan diperkenalkan pada tahun 2018. Ini menawarkan peningkatan keamanan yang signifikan dibandingkan dengan WPA2, termasuk perlindungan yang lebih baik terhadap serangan brute-force dan peningkatan privasi pada jaringan terbuka. Namun, WPA3 membutuhkan perangkat keras yang kompatibel dan belum sepenuhnya diadopsi.

7.3.5 Lainnya (TKIP, AES, etc.)

TKIP dan AES adalah metode enkripsi yang digunakan oleh protokol keamanan WPA dan WPA2. Seperti disebutkan sebelumnya, TKIP digunakan oleh WPA dan AES digunakan oleh WPA2. Selain itu, ada juga metode enkripsi lain seperti Blowfish dan RSA, tetapi mereka umumnya tidak digunakan dalam konteks jaringan Wi-Fi.

Untuk keamanan optimal, umumnya disarankan untuk menggunakan WPA2 atau WPA3 (jika didukung oleh perangkat keras Anda) dengan AES. Jangan gunakan WEP atau WPA dengan TKIP, karena mereka memiliki kelemahan keamanan yang signifikan.

7.4 Alat dan Teknik Keamanan Wireless

7.4.1 Firewall dan Intrusion Prevention Systems

Firewall berfungsi sebagai penghalang antara jaringan internal yang dipercaya dan jaringan luar yang tidak dipercaya, seperti internet. Firewall dapat menginspeksi lalu lintas jaringan dan memblokir lalu lintas yang mencurigakan atau yang tidak

diizinkan berdasarkan serangkaian aturan yang ditentukan sebelumnya.

Intrusion Prevention Systems (IPS), di sisi lain, adalah sistem keamanan jaringan yang memantau lalu lintas jaringan untuk mencari tanda-tanda aktivitas jahat yang bisa menjadi indikasi serangan cyber. Jika aktivitas mencurigakan dideteksi, IPS dapat mengambil tindakan untuk menghentikan serangan tersebut.

7.4.2 *Virtual Private Networks* (VPNs)

VPN adalah teknologi yang memungkinkan pengguna untuk membuat koneksi internet yang aman dan pribadi, bahkan saat menggunakan jaringan yang tidak aman, seperti Wi-Fi publik. VPN bekerja dengan mengenkripsi data yang dikirim dan diterima oleh pengguna, sehingga orang lain tidak dapat memata-matai atau mengganggu koneksi tersebut.

7.4.3 *Network Access Control* (NAC)

NAC adalah pendekatan untuk keamanan jaringan yang melibatkan membatasi akses ke jaringan berdasarkan identitas dan kepatuhan perangkat terhadap kebijakan keamanan. Misalnya, NAC dapat digunakan untuk memastikan bahwa hanya perangkat yang telah terdaftar dan memenuhi kebijakan keamanan tertentu (seperti memiliki antivirus terbaru) yang diizinkan untuk mengakses jaringan.

7.4.4 *Wireless Intrusion Prevention Systems* (WIPS)

WIPS adalah sistem yang dirancang khusus untuk memantau, mendeteksi, dan mencegah akses yang tidak sah ke jaringan nirkabel. WIPS bekerja dengan memantau spektrum nirkabel untuk aktivitas yang mencurigakan, seperti perangkat yang mencoba untuk menyambungkan ke jaringan tanpa otorisasi, dan dapat mengambil tindakan untuk mencegah akses tersebut.

7.5 Praktik Terbaik Keamanan Wireless

7.5.1 Mendefinisikan Kebijakan Keamanan Wireless

Sebagai langkah pertama, penting untuk mendefinisikan dan menerapkan kebijakan keamanan wireless yang jelas. Kebijakan ini harus mencakup aspek seperti siapa yang berhak mengakses jaringan, jenis perangkat yang diperbolehkan, dan standar enkripsi yang harus digunakan.

7.5.2 Menggunakan Enkripsi Kuat

Seperti yang telah dibahas sebelumnya, menggunakan protokol enkripsi yang kuat seperti WPA2 atau WPA3 dengan AES sangat penting untuk menjaga keamanan jaringan nirkabel. Ini akan membantu melindungi data Anda dari penyadapan dan akses yang tidak sah.

7.5.3 Mengubah Default SSID dan Password

Banyak perangkat jaringan nirkabel datang dengan nama jaringan (SSID) dan password default yang umum diketahui. Oleh karena itu, penting untuk mengubah baik SSID dan password menjadi sesuatu yang unik dan sulit ditebak.

7.5.4 Menyembunyikan SSID

Menyembunyikan SSID - atau membuat nama jaringan Anda tidak terlihat untuk orang lain - dapat membantu mengurangi risiko akses yang tidak sah. Meski tidak sepenuhnya membuat jaringan Anda kebal dari serangan, ini bisa menambah lapisan ekstra keamanan.

7.5.5 Mengaktifkan MAC Address Filtering

Setiap perangkat yang terhubung ke jaringan memiliki alamat MAC yang unik. Dengan mengaktifkan fitur filtering alamat MAC, Anda dapat mengatur jaringan Anda sehingga hanya perangkat dengan alamat MAC tertentu yang diizinkan untuk

terhubung. Ini dapat membantu mencegah akses yang tidak sah, meski perlu diperhatikan bahwa metode ini bisa menjadi beban administratif jika Anda memiliki banyak perangkat, dan tidak memberikan perlindungan penuh, karena alamat MAC bisa dipalsukan.

7.6 Ancaman dan Serangan Keamanan Wireless Terkini

7.6.1 *Eavesdropping* dan *Interception*

Eavesdropping dan *Interception* adalah ancaman di mana pelaku mendengarkan atau mencegat komunikasi nirkabel untuk mendapatkan akses ke data yang sensitif. Teknologi nirkabel secara alamiah lebih rentan terhadap jenis serangan ini karena data disiarkan melalui udara dan dapat diintersep oleh siapa saja yang berada dalam jangkauan.

7.6.2 *Man-In-The-Middle Attacks*

Man-In-The-Middle (MITM) Attacks adalah ancaman di mana pelaku menempatkan diri mereka di antara dua pihak yang sedang berkomunikasi. Dengan demikian, mereka dapat mencegat dan memodifikasi komunikasi tersebut. Pelaku dapat menggunakan teknik seperti ARP *spoofing* atau rogue access points untuk melancarkan serangan MITM di jaringan nirkabel.

7.6.3 *Denial of Service* (DoS) *Attacks*

Serangan *Denial of Service* (DoS) adalah upaya untuk membuat suatu sumber daya (seperti jaringan, server, atau aplikasi) tidak dapat digunakan oleh pengguna yang sah. Dalam konteks jaringan nirkabel, serangan DoS dapat dilakukan dengan berbagai cara, seperti membanjiri jaringan dengan lalu lintas yang tidak perlu atau menggunakan teknik seperti *deauthentication attacks.*

7.6.4 Network Injection Attacks

Network Injection adalah jenis serangan di mana pelaku memasukkan paket atau data berbahaya ke dalam jaringan nirkabel. Jika paket ini diterima dan diproses oleh perangkat target, mereka dapat menyebabkan berbagai masalah, mulai dari gangguan kinerja hingga pelanggaran keamanan yang serius. Perangkat yang tidak aman atau konfigurasi jaringan yang tidak tepat dapat mempermudah serangan injeksi jaringan.

7.7 Masa Depan Keamanan Wireless

7.7.1 Perkembangan Teknologi Terbaru

Teknologi wireless terus berkembang dengan cepat, dan ini tentu akan berdampak pada keamanan wireless. Misalnya, teknologi 5G dan Wi-Fi 6 menawarkan peningkatan kecepatan dan kapasitas yang signifikan, tetapi juga menimbulkan tantangan keamanan baru yang harus diatasi. Selain itu, IoT (Internet of Things), di mana semakin banyak perangkat terhubung ke internet, juga membuka peluang baru bagi ancaman dan serangan keamanan.

Dalam konteks protokol keamanan, standar baru seperti WPA3 dan Enhanced Open telah diperkenalkan untuk mengatasi kelemahan dalam protokol keamanan sebelumnya dan memberikan perlindungan yang lebih baik terhadap serangan. Namun, penerapan protokol baru ini memerlukan perangkat keras yang kompatibel dan dapat membutuhkan investasi yang signifikan.

7.7.2 Tantangan dan Peluang

Seiring dengan perkembangan teknologi wireless, tantangan keamanan juga berkembang. Ancaman keamanan baru terus muncul, dan organisasi harus tetap up-to-date dengan tren keamanan terkini untuk melindungi jaringan mereka. Peningkatan

penggunaan mobile dan remote work juga menimbulkan tantangan keamanan yang unik yang harus diatasi.

Di sisi lain, perkembangan ini juga membuka peluang baru. Misalnya, teknologi AI dan machine learning dapat digunakan untuk mendeteksi ancaman keamanan dengan lebih efektif dan meresponsnya dengan lebih cepat. Selain itu, adopsi solusi cloud dan *as-a-service* dapat memungkinkan organisasi untuk memanfaatkan keahlian dan infrastruktur keamanan dari penyedia layanan khusus, sehingga mengurangi beban internal dan memungkinkan mereka untuk fokus pada inti bisnis mereka.

7.8 Studi Kasus

7.8.1 Kasus Pelanggaran Keamanan Wireless

Pelanggaran keamanan wireless dapat berdampak besar pada organisasi dan individu. Misalnya, pada tahun 2017, perusahaan perangkat lunak besar bernama Equifax mengalami pelanggaran data yang mempengaruhi hampir 148 juta orang. Meskipun serangan ini bukan secara langsung melalui jaringan wireless, ini menunjukkan dampak dari pelanggaran keamanan pada skala besar.

Sebuah contoh lain melibatkan serangan terhadap hotel St. Regis di Shanghai pada tahun 2014. Dalam kasus ini, penyerang berhasil menyerang jaringan Wi-Fi hotel untuk mendapatkan akses ke sistem manajemen tamu hotel. Ini memungkinkan mereka untuk melihat detail pribadi tamu dan bahkan membuka pintu kamar.

7.8.2 Solusi dan Pelajaran yang Dapat Dipetik

Setiap pelanggaran keamanan adalah peluang untuk belajar dan memperbaiki keamanan jaringan. Dalam kasus Equifax, salah satu pelajaran utama adalah pentingnya memperbarui dan memperbaiki perangkat lunak yang rentan. Equifax telah menunda

memperbarui perangkat lunak yang mereka ketahui rentan, yang akhirnya mengarah pada pelanggaran.

Dalam kasus St. Regis Shanghai, serangan tersebut menunjukkan pentingnya keamanan jaringan hotel dan bisnis lainnya yang menangani data pelanggan. Selain menggunakan enkripsi dan otentikasi yang kuat, perusahaan harus mempertimbangkan untuk menggunakan jaringan terpisah untuk sistem manajemen dan jaringan tamu untuk mencegah akses yang tidak sah ke sistem penting.

Untuk kedua kasus, solusi melibatkan peningkatan pendidikan dan kesadaran tentang keamanan, serta adopsi praktik terbaik seperti pembaruan dan pemeliharaan rutin, dan menggunakan teknologi keamanan terkini.

7.9 Kesimpulan

Keamanan wireless adalah aspek penting dalam dunia yang semakin digital dan terkoneksi. Baik pada tingkat individual maupun organisasional, perlindungan data dan informasi penting sangatlah esensial. Perkembangan teknologi wireless telah membawa banyak manfaat, seperti kenyamanan dan fleksibilitas, tetapi juga menimbulkan tantangan dan ancaman keamanan yang baru dan semakin kompleks.

Melalui pemahaman yang baik tentang dasar-dasar keamanan wireless, protokol dan alat yang digunakan, serta ancaman dan serangan yang mungkin terjadi, kita dapat lebih siap untuk melindungi diri kita sendiri dan organisasi kita. Penerapan praktik terbaik keamanan, seperti penggunaan enkripsi yang kuat, mengubah default SSID dan password, dan menyembunyikan SSID, dapat secara signifikan mengurangi risiko.

Meski begitu, penting juga untuk memahami bahwa tidak ada sistem yang sepenuhnya aman. Oleh karena itu, selalu penting untuk tetap berjaga-jaga dan up-to-date dengan perkembangan terbaru dalam teknologi dan keamanan wireless. Menyadari

potensi ancaman, dan memiliki rencana respons yang baik jika terjadi pelanggaran, juga sangat penting.

Dalam konteks masa depan, meskipun ada tantangan yang akan datang seiring dengan perkembangan teknologi seperti 5G, Wi-Fi 6, dan IoT, juga ada peluang untuk menggunakan teknologi baru seperti AI dan cloud untuk meningkatkan keamanan. Seperti halnya dalam banyak aspek teknologi, adaptasi dan pembelajaran berkelanjutan adalah kunci untuk keberhasilan.

DAFTAR PUSTAKA

Stallings, W., & Brown, L. 2018. Computer security: principles and practice. Pearson.

Scarfone, K., & Chen, L. 2013. Guide to securing legacy IEEE 802.11 wireless networks. NIST Special Publication, 800-48, Rev. 1.

Bhagwat, P., Bhattacharya, P., Krishna, A., & Tripathi, S. K. 2004. Enhancing throughput over wireless LAN by traffic shaping. In Proceeding IEEE International Conference on Networking, ICN 2004.

Ogun, S. 2016. The threats to our Wi-Fi have changed: Should our security? Network Security, 2016(3), 5-7.

Deng, J., Han, R., & Mishra, S. 2005. Defending against path-based DoS attacks in wireless sensor networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks.

Vanhoef, M., & Piessens, F. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Geier, E. 2016. Wireless Network Security for Beginners. Computerworld. Retrieved from www.computerworld.com.

Singh, S., & Singh, P. 2014. Study of WPA and 802.11i security protocols. In Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

Gast, M. 2005. 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media.

BAB 8
WEB SECURITY

Oleh Yendi Putra

8.1 Pendahuluan

Website adalah kumpulan halaman web yang terhubung satu sama lain dan dapat diakses melalui Internet. Website telah menjadi bagian penting dari kehidupan kita sehari-hari dan berperan dalam menyediakan informasi, memfasilitasi interaksi, dan menghubungkan orang-orang di seluruh dunia. Dalam era digital saat ini, hampir setiap individu, perusahaan, organisasi, atau institusi memiliki website sebagai sarana komunikasi dan kehadiran online. Pada dasarnya, website terdiri dari beberapa elemen penting, termasuk halaman web, konten, tautan, gambar, video, dan fitur interaktif. Halaman web adalah unit dasar dari sebuah website, dan setiap halaman dapat berisi teks, gambar, dan elemen-elemen lainnya yang ditampilkan dalam tata letak yang terstruktur. Konten website meliputi informasi, artikel, blog, produk, layanan, dan segala macam materi yang disajikan kepada pengguna. (Iqbal Kurniansyah & Sinurat, 2020).

Website juga memiliki tautan yang menghubungkan halaman-halaman web yang berbeda, memungkinkan pengguna untuk menjelajahi dan berpindah dari satu halaman ke halaman lainnya dengan mudah. Tautan ini juga memungkinkan pengguna untuk berinteraksi dengan website, mengikuti navigasi, mengisi formulir, atau melakukan tindakan lainnya. Website juga dapat berisi berbagai jenis media seperti gambar dan video. Gambar digunakan untuk memperkaya konten dan menarik perhatian pengguna, sementara video memberikan pengalaman multimedia yang lebih interaktif dan menarik.

Gambar 8.1. Pengenalan Website
Sumber: https://www.indoworx.com

Fitur interaktif pada website memungkinkan pengguna untuk berpartisipasi secara aktif. Misalnya, pengguna dapat mengisi formulir, mengirim komentar, membagikan konten ke media sosial, atau berinteraksi dengan elemen-elemen interaktif lainnya. Fitur ini membantu dalam membangun hubungan yang lebih dekat antara pengguna dan pemilik website serta mendorong interaksi lebih lanjut.

Manfaat utama dari memiliki website adalah dapat menjangkau audiens yang lebih luas dan menyediakan informasi yang mudah diakses. Website dapat diakses oleh siapa saja, kapan saja, dan dari mana saja dengan menggunakan perangkat yang terhubung ke Internet. Dengan demikian, website memberikan fleksibilitas dan aksesibilitas yang tinggi. Selain itu, website juga dapat digunakan untuk membangun merek atau identitas online. Website dapat mencerminkan identitas, nilai-nilai, dan tujuan

organisasi atau individu. Dengan desain yang sesuai dan konten yang relevan, website dapat memberikan kesan yang baik kepada pengguna dan membangun kepercayaan.Website juga dapat digunakan untuk tujuan komersial.

8.1.1 Perkembangan Website:

Pada awalnya, website hanya terdiri dari halaman-halaman statis yang ditampilkan secara sederhana dengan teks dan gambar. Mereka dirancang menggunakan HTML (*Hypertext Markup Language*), yaitu bahasa pemrograman yang digunakan untuk membuat struktur dasar dan tampilan halaman web. Kemudian, dengan munculnya CSS (*Cascading Style Sheets*), website dapat lebih mudah diatur tampilannya dan diberikan gaya yang konsisten.

Seiring dengan perkembangan internet dan teknologi, website menjadi lebih dinamis dan interaktif. Teknologi pemrograman seperti JavaScript mulai digunakan untuk memberikan fungsi interaktif pada halaman web, seperti validasi formulir, animasi, dan interaksi pengguna. Ini membawa pengalaman pengguna yang lebih baik dan memungkinkan website untuk melakukan tugas yang lebih kompleks.

Selanjutnya, munculnya platform CMS (*Content Management System*) seperti WordPress, Joomla, dan Drupal memudahkan pembuatan dan pengelolaan website. CMS menyediakan antarmuka yang intuitif dan memungkinkan pengguna untuk mengatur konten, mengubah tampilan, dan menambahkan fitur dengan mudah, tanpa harus memiliki pengetahuan pemrograman yang mendalam.(Herdiana & Saepudin, 2023)

8.1.2 Teknologi yang digunakan dalam membangun sebuah website:

Untuk menghadirkan website yang lebih dinamis, teknologi seperti *server-side scripting* digunakan. *Server-side scripting*

memungkinkan penggunaan bahasa pemrograman seperti PHP, *Python*, dan *Ruby* untuk memproses data dan menghasilkan konten secara dinamis sebelum dikirim ke pengguna. Ini memungkinkan website untuk menyediakan konten yang disesuaikan, seperti menampilkan hasil pencarian, memproses formulir, atau mengakses basis data.

Selain itu, penggunaan database juga penting dalam pengembangan website. Basis data seperti MySQL, PostgreSQL, dan MongoDB digunakan untuk menyimpan dan mengelola informasi yang diperlukan oleh website, seperti profil pengguna, entri blog, atau data produk. (Haryanto, 2017) Selama beberapa tahun terakhir, ada juga perkembangan teknologi frontend yang signifikan. Framework dan library JavaScript seperti React, Angular, dan Vue.js memungkinkan pengembang untuk membangun antarmuka pengguna yang responsif, interaktif, dan menarik dengan lebih efisien. Website dapat dibangun menggunakan berbagai teknologi dan bahasa pemrograman, seperti HTML (*Hypertext Markup Language*), CSS (*Cascading Style Sheets*), JavaScript, dan PHP (*Hypertext Preprocessor*). Ada juga platform manajemen konten (*content management systems*) seperti WordPress, Joomla, atau Drupal yang memudahkan pembuatan dan pengelolaan website tanpa harus memiliki pengetahuan pemrograman yang mendalam.

Dengan munculnya teknologi web yang semakin maju, seperti responsif web design (*desain web responsif*), website juga dapat diakses melalui berbagai perangkat, seperti komputer desktop, laptop, tablet, dan ponsel pintar, dengan tampilan yang sesuai dengan ukuran layar perangkat yang digunakan. Secara umum, website adalah sebuah wadah di dunia maya yang menyajikan konten dan memungkinkan interaksi dengan pengguna melalui internet.

8.2 Jenis-jenis website

Website memiliki beberapa jenis diantaranya:

1. Website Informasi: Jenis website ini dirancang untuk memberikan informasi kepada pengguna. Contohnya adalah situs berita, blog, ensiklopedia online, dan portal informasi.
2. Website E-Commerce: Website e-commerce digunakan untuk melakukan transaksi jual beli online. Ini termasuk toko online, pasar online, atau platform e-commerce yang memfasilitasi pembelian produk atau layanan secara elektronik.
3. Website Pendidikan: Website pendidikan berfokus pada penyediaan konten pendidikan, sumber belajar, kursus online, atau platform e-learning.
4. Website Hiburan: Jenis website ini menyajikan konten hiburan seperti streaming musik, film, video, permainan online, dan platform sosial media.
5. Website Blog dan Personal: Website blog dan personal digunakan oleh individu untuk berbagi pemikiran, pengalaman, dan karya mereka dengan pembaca. Ini bisa berupa blog pribadi, portofolio profesional, atau situs web untuk mempromosikan karya seni dan kreatifitas.
6. Website Sosial Media: Website sosial media adalah platform yang memungkinkan pengguna untuk terhubung, berinteraksi, dan berbagi konten dengan orang lain secara online. Contohnya adalah Facebook, Twitter, Instagram, LinkedIn, dan lain sebagainya.
7. Website Institusi dan Organisasi: Website ini dimiliki oleh institusi, organisasi, atau lembaga tertentu, seperti pemerintah, sekolah, universitas, organisasi nirlaba, atau perusahaan. Tujuannya adalah untuk menyediakan informasi tentang lembaga tersebut, layanan yang ditawarkan, dan berinteraksi dengan pengguna.

8. Website Forum dan Komunitas: Jenis website ini digunakan untuk membentuk komunitas online, di mana pengguna dapat berinteraksi, berbagi ide, dan berdiskusi tentang topik-topik tertentu. Contoh dari website ini adalah Reddit atau Stack Overflow.
9. Website Media Streaming: Website media streaming menyediakan konten audio atau video yang dapat diakses secara langsung melalui internet. Contohnya adalah platform streaming musik seperti Spotify atau platform streaming video seperti YouTube atau Netflix.
10. Website Pemerintah: Website pemerintah digunakan oleh instansi pemerintah untuk menyediakan informasi tentang pemerintahan, layanan publik, undang-undang, dan interaksi dengan warga negara.

8.3 Bahasa pemrograman yang digunakan membuat website:

Website dibangun dengan menggunakan bahasa pemrograman diantaranya:

1. HTML (*Hypertext Markup Language*): HTML adalah bahasa markah yang digunakan untuk membangun struktur dan konten dasar sebuah halaman web. Ini adalah bahasa dasar yang digunakan dalam hampir setiap website.
2. CSS (*Cascading Style Sheets*): CSS digunakan untuk mengatur tampilan dan tata letak halaman web. Dengan CSS, Anda dapat mengontrol warna, ukuran, jenis font, margin, padding, dan elemen visual lainnya pada halaman web.
3. JavaScript: JavaScript adalah bahasa pemrograman yang digunakan untuk membuat halaman web interaktif dan dinamis. Dengan JavaScript, Anda dapat menambahkan fungsionalitas seperti validasi form, animasi, efek visual, interaksi pengguna, dan masih banyak lagi.

4. PHP (*Hypertext Preprocessor*): PHP adalah bahasa pemrograman yang biasanya digunakan untuk mengembangkan bagian server-side dari website. PHP berfungsi untuk memproses data dari pengguna, berinteraksi dengan basis data, dan menghasilkan konten dinamis yang akan ditampilkan di halaman web.
5. *Python*: *Python* adalah bahasa pemrograman serbaguna yang juga dapat digunakan untuk pengembangan web. Dengan kerangka kerja web seperti Django atau Flask, Anda dapat membuat aplikasi web yang kuat dan skala besar dengan Python.
6. *Ruby*: *Ruby* adalah bahasa pemrograman yang populer digunakan dalam pengembangan web, terutama dengan kerangka kerja *Ruby on Rails*. *Ruby on Rails* mempermudah pembuatan aplikasi web dengan menyediakan banyak fitur dan konvensi yang membantu dalam pengembangan cepat dan efisien.
7. Java: Java adalah bahasa pemrograman yang sering digunakan dalam pengembangan web, terutama untuk pembuatan aplikasi berbasis enterprise dan perusahaan. Java dapat digunakan dengan kerangka kerja seperti Spring untuk membangun aplikasi web yang skalabel dan aman.
8. C#: C# adalah bahasa pemrograman yang sering digunakan dalam pengembangan aplikasi web berbasis Microsoft. Dengan kerangka kerja seperti ASP.NET, Anda dapat membuat aplikasi web yang kuat dan berkinerja tinggi menggunakan C#.

8.4 Domain dan Hosting

8.4.1 Domain

Domain merujuk pada alamat unik yang digunakan untuk mengidentifikasi dan mengakses sebuah website di internet. Dalam istilah yang lebih teknis, domain adalah bagian dari URL (*Uniform*

Resource Locator) yang digunakan untuk menentukan alamat spesifik dari suatu halaman web atau sumber daya lainnya di internet.

Sebuah domain terdiri dari dua komponen utama: nama domain dan ekstensi domain. Nama domain adalah bagian yang dapat dipilih oleh pemilik website dan mewakili identitas atau tujuan dari website tersebut. Misalnya, dalam "www.example.com", "example" adalah nama domain. Ekstensi domain adalah bagian yang terletak setelah nama domain dan menunjukkan jenis atau kategori dari website tersebut. Contohnya, dalam "www.example.com", "com" adalah ekstensi domain.

Berikut ini adalah beberapa contoh ekstensi domain yang umum digunakan:

1. .com (komersial) - digunakan untuk bisnis komersial dan organisasi di seluruh dunia.
2. .org (organisasi) - digunakan untuk organisasi non-profit dan nirlaba.
3. .net (jaringan) - digunakan untuk organisasi yang terkait dengan jaringan dan infrastruktur internet.
4. .edu (pendidikan) - digunakan untuk institusi pendidikan tinggi dan lembaga pendidikan.
5. .gov (pemerintah) - digunakan untuk entitas pemerintah.
6. .mil (militer) - digunakan untuk departemen militer suatu negara.
7. .info (informasi) - digunakan untuk situs web yang memberikan informasi.
8. .biz (bisnis) - digunakan untuk bisnis dan perusahaan.
9. .co (company) - digunakan untuk bisnis dan perusahaan.
10. .me (personal) - digunakan untuk situs web personal.
11. .io (input/output) - sering digunakan oleh perusahaan teknologi dan startup.

12. .dev (pengembangan) - digunakan untuk situs web yang berkaitan dengan pengembangan perangkat lunak dan teknologi.
13. .shop (belanja) - digunakan untuk situs web yang berhubungan dengan perdagangan dan belanja online.
14. .blog (blog) - digunakan untuk situs web blog.
15. .tv (televisi) - sering digunakan oleh situs web dan platform yang berfokus pada konten video.

Domain dapat dibeli atau didaftarkan melalui registrar domain yang berwenang. Setelah mendaftarkan domain, pemilik website memiliki hak eksklusif untuk menggunakan nama domain tersebut dan mengarahkannya ke server tempat website di-hosting. Selain sebagai alamat unik, domain juga memiliki peran penting dalam membentuk identitas online sebuah website dan memudahkan pengguna untuk mengingat dan mengakses website tersebut dengan mudah. (Ramaddan Julianti *et al.,* 2022)

8.4.2 Hosting

Hosting merujuk pada layanan yang menyediakan ruang penyimpanan dan aksesibilitas bagi sebuah website di internet. Ketika Anda membuat sebuah website, semua file, data, gambar, dan konten yang terkait dengan website tersebut harus disimpan di sebuah server yang terhubung ke internet. Server tersebut akan menyimpan dan mengirimkan informasi yang diperlukan ketika website diakses oleh pengguna.

Hosting web adalah proses menyewa atau membeli ruang server dari penyedia hosting web untuk menyimpan semua file dan data website Anda. Penyedia hosting web akan menyediakan infrastruktur server, konektivitas internet, dan layanan yang diperlukan untuk menjaga website Anda tetap online dan dapat diakses oleh pengguna di seluruh dunia. (Utami Aulia Alma, 2018)

Sebagai pelanggan hosting, Anda akan mendapatkan alamat IP (*Internet Protocol*) yang unik atau nama domain yang akan digunakan untuk mengarahkan pengguna ke server tempat website Anda di-hosting. Pengguna kemudian dapat mengakses website Anda melalui browser mereka dengan memasukkan alamat domain atau URL yang sesuai.

Gambar 8.12. Ilustrasi Hosting
Sumber: https://pasca.uma.ac.id/

Ada beberapa jenis hosting web yang tersedia diantaranya:

1. *Shared Hosting*: Dalam *shared hosting*, beberapa website yang berbeda akan di-hosting di server yang sama. Sumber daya server, seperti ruang penyimpanan, bandwidth, dan daya pemrosesan, dibagi di antara banyak pengguna. Ini adalah pilihan yang umum dan terjangkau untuk website kecil atau pemula.
2. VPS Hosting: *Virtual Private Server* (VPS) adalah bentuk hosting di mana server fisik dibagi menjadi beberapa server virtual yang beroperasi secara independen. Setiap

VPS memiliki sumber daya yang terisolasi dan lebih fleksibel daripada shared hosting.

3. *Dedicated Hosting*: Dalam *dedicated hosting*, Anda memiliki server fisik secara eksklusif untuk website Anda sendiri. Ini memberikan akses penuh terhadap semua sumber daya server dan memberikan kinerja terbaik. *Dedicated hosting* cocok untuk website dengan lalu lintas tinggi atau kebutuhan khusus.
4. *Cloud Hosting*: *Cloud hosting* menggunakan infrastruktur cloud computing untuk menyediakan ruang server yang fleksibel dan skalabel. Sumber daya server didistribusikan di berbagai server fisik di berbagai lokasi, dan website Anda dapat memanfaatkan sumber daya tersebut sesuai kebutuhan.
5. *Managed Hosting*: Dalam managed hosting, penyedia hosting web mengelola server dan tugas-tugas teknis terkait seperti pemeliharaan, pembaruan keamanan, dan backup data. Ini memungkinkan Anda untuk fokus pada pengembangan dan konten website Anda, sementara penyedia hosting mengurus aspek teknisnya.

Pemilihan jenis hosting web yang tepat tergantung pada ukuran dan kebutuhan website Anda, tingkat lalu lintas yang diharapkan, tingkat kendali dan akses yang Anda butuhkan, serta anggaran yang tersedia

Berikut adalah beberapa penyedia layanan hosting di Indonesia:

1. Niagahoster (https://www.niagahoster.co.id/)
2. Rumahweb (https://www.rumahweb.com/)
3. Hostinger (https://www.hostinger.co.id/)
4. IDCloudHost (https://www.idcloudhost.com/)
5. Qwords (https://www.qwords.com/)
6. Dewaweb (https://www.dewaweb.com/)

7. Jagoan Hosting (https://www.jagoanhosting.com/)
8. DomaiNesia (https://www.domainesia.com/)
9. Ardhosting (https://www.ardhosting.com/)
10. Hostnet (https://www.hostnet.co.id/)

8.5 Pendekatan atau Metodologi dalam Melakukan Pentrationtest Website

Ada beberapa jenis pendekatan yang umum digunakan dalam pengujian penetrasi (penetration testing) untuk mengidentifikasi kelemahan keamanan dalam sistem. Berikut ini beberapa jenis pendekatan yang umum digunakan:

1. *Black Box Testing*: Dalam pendekatan ini, penyerang (*penetration tester*) tidak memiliki pengetahuan sebelumnya tentang sistem yang akan diuji. Mirip dengan black box hacking, penyerang akan mencoba mendapatkan akses tidak sah ke sistem dengan sedikit atau tanpa pengetahuan rinci tentang infrastruktur, arsitektur, atau kode sumber sistem. Hal ini membantu untuk mensimulasikan serangan dari pihak luar yang tidak memiliki pengetahuan internal sistem. (Salamah, U., & Khasanah, 2017)
2. *White Box Testing*: Dalam pendekatan ini, penyerang memiliki pengetahuan yang lengkap tentang sistem yang akan diuji. Penyerang memiliki akses ke kode sumber, dokumentasi, dan informasi rinci lainnya tentang sistem target. Dengan pengetahuan ini, penyerang dapat melakukan analisis keamanan secara mendalam, termasuk mengaudit kode sumber, menganalisis konfigurasi sistem, dan mencari celah keamanan. (Sie e*t al.*, 2022)
3. *Grey Box Testing*: Pendekatan ini berada di antara *black box* dan *white box testing*. Penyerang memiliki sebagian pengetahuan tentang sistem yang akan diuji, seperti beberapa informasi konfigurasi atau dokumentasi terbatas.

Dengan informasi tersebut, penyerang dapat mengarahkan upaya *hacking* mereka ke area yang lebih mungkin rentan. Pendekatan *grey box testing* mencoba memadukan keuntungan dari *black box* dan *white box testing*. (Wang *et al.*, 2020)

4. *External Testing*: Pendekatan ini melibatkan penyerangan dari sisi eksternal atau luar jaringan. Penyerang mencoba menemukan celah keamanan dari luar jaringan yang melibatkan serangan dari Internet. Ini mencakup pengujian seperti port scanning, penilaian rentang IP, serangan DDoS, dan mencari kelemahan pada perimeter jaringan.
5. *Internal Testing*: Pendekatan ini melibatkan penyerangan dari sisi internal jaringan. Penyerang mencoba mendapatkan akses ke jaringan internal dan melakukan serangan terhadap sistem dari dalam jaringan. Hal ini mencakup pengujian seperti mencoba mendapatkan akses yang tidak sah ke sistem yang dilindungi dengan firewall, melakukan serangan privilege escalation, atau mencari kelemahan pada sistem internal.
6. *Blind Testing*: Pendekatan ini mensimulasikan serangan di mana penyerang memiliki sedikit atau tanpa informasi sebelumnya tentang sistem yang akan diuji. Ini menguji kemampuan tim keamanan dalam mendeteksi, melacak, dan merespons serangan yang tidak terduga.
7. *Double-Blind Testing*: Pendekatan ini mirip dengan blind testing, tetapi dengan tambahan bahwa tim keamanan tidak memiliki pengetahuan tentang pendekatan pengujian yang digunakan. Ini dirancang untuk mengevaluasi kemampuan tim keamanan dalam menghadapi serangan yang tidak diketahui dengan sedikit atau tanpa persiapan sebelumnya.

Setiap pendekatan memiliki kelebihan dan kelemahan masing-masing dan dapat dipilih berdasarkan kebutuhan dan tujuan pengujian keamanan yang diinginkan.

8.6 Jenis-Jenis Serangan Pada Website

8.6.1 Serangan SQL Injection

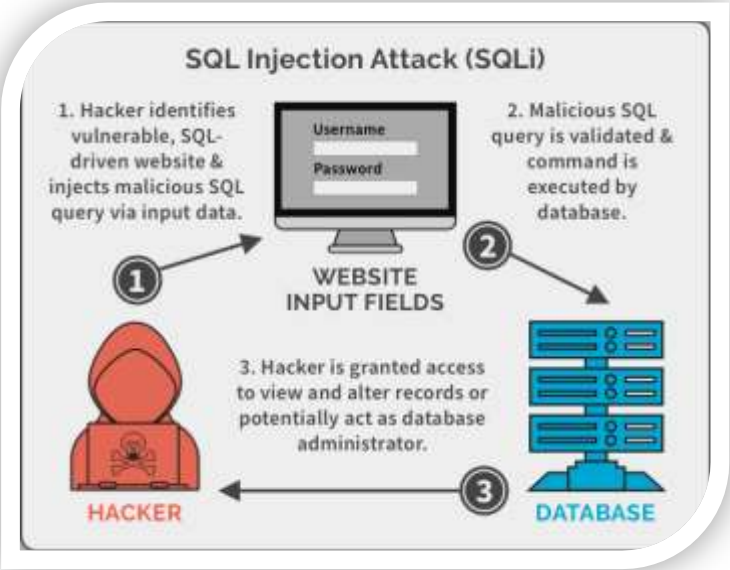
Serangan SQL *Injection*: Serangan SQL Injection adalah jenis serangan yang dilakukan dengan menyisipkan kode SQL berbahaya ke dalam input yang diterima oleh aplikasi web. Jika aplikasi tidak memvalidasi atau mengelola input dengan benar, serangan SQL Injection dapat memungkinkan penyerang untuk mengeksekusi perintah SQL yang tidak sah atau memanipulasi perintah SQL yang ada. (Alanda *et al.*, 2021)

Dampak negatif serangan SQL Injection diantaranya:

1. Pengungkapan Data Sensitif: Dalam serangan SQL *Injection*, penyerang dapat mengambil, membaca, atau mengungkapkan data sensitif yang tersimpan dalam database, seperti informasi pengguna, informasi kartu kredit, atau data rahasia lainnya. Ini dapat mengakibatkan pelanggaran privasi yang serius dan berpotensi merugikan pengguna atau organisasi yang terkena dampak.
2. Manipulasi atau Penghapusan Data: Serangan SQL *Injection* juga memungkinkan penyerang untuk memanipulasi, mengubah, atau menghapus data dalam database. Penyerang dapat mengubah informasi penting, merusak integritas data, atau bahkan menghapus keseluruhan database. Dampaknya bisa berupa kerugian finansial, kerugian reputasi, atau gangguan operasional yang signifikan.
3. Eksekusi Kode Berbahaya: Serangan SQL Injection dapat memungkinkan penyerang untuk menyisipkan kode berbahaya, seperti skrip JavaScript atau perintah sistem operasi, yang akan dieksekusi oleh aplikasi web atau

browser pengguna. Ini dapat digunakan untuk melakukan serangan lain, mencuri informasi, atau mengambil kontrol penuh atas sistem yang diserang.

4. Pemutusan Layanan: Serangan SQL Injection yang berhasil dapat membebani server atau sistem yang diserang dengan beban yang berlebihan, menyebabkan penurunan kinerja atau bahkan pemutusan layanan (*denial of service*). Hal ini dapat mengganggu operasional bisnis, mengakibatkan hilangnya peluang bisnis, atau menyebabkan ketidaknyamanan bagi pengguna.



Gambar 8.13. Cara Hacker Melakukan Serangan SQL Injection
Sumber: https://spanning.com/

Salah satu kasus besar yang melibatkan serangan SQL Injection adalah serangan pada situs e-commerce terkenal yang dikenal sebagai serangan Heartland Payment Systems pada tahun

2008. Heartland Payment Systems adalah perusahaan pemrosesan pembayaran yang bertanggung jawab untuk memproses transaksi kartu kredit bagi ribuan bisnis di Amerika Serikat.

Serangan ini dilakukan oleh hacker yang dikenal dengan nama Albert Gonzalez dan kelompoknya. Mereka berhasil menginfeksi sistem Heartland Payment Systems dengan menyisipkan kode berbahaya melalui serangan SQL Injection. Serangan tersebut memungkinkan mereka untuk mencuri data kartu kredit yang terproses oleh perusahaan.

Dampaknya sangat besar, karena serangan ini mengakibatkan pencurian data kartu kredit dari jutaan pelanggan yang menggunakan layanan Heartland Payment Systems. Data yang dicuri termasuk nomor kartu kredit, nama pemilik kartu, tanggal kedaluwarsa, dan data terkait lainnya. Serangan ini dianggap sebagai salah satu serangan terbesar dalam sejarah keamanan data, dan mempengaruhi banyak perusahaan dan individu di seluruh dunia.

Kasus Heartland Payment Systems menjadi peringatan penting tentang seriusnya ancaman SQL Injection dan pentingnya menjaga keamanan aplikasi web. Hal ini mendorong organisasi untuk meningkatkan langkah-langkah keamanan mereka dan meningkatkan kesadaran tentang praktik pengembangan yang aman untuk melindungi data sensitif pengguna.

Berikut adalah langkah-langkah umum yang terjadi dalam serangan SQL *Injection:*

1. Identifikasi Poin Rentan: Penyerang mencari celah keamanan pada aplikasi web yang memungkinkan mereka menyisipkan input yang tidak divalidasi secara benar ke dalam perintah SQL.
2. Mendeteksi Struktur Database: Penyerang mencoba untuk mengidentifikasi struktur database yang digunakan oleh aplikasi, termasuk tabel, kolom, dan nama field. Ini bisa

dilakukan dengan menganalisis respons dari aplikasi atau dengan menggunakan teknik seperti komentar SQL.

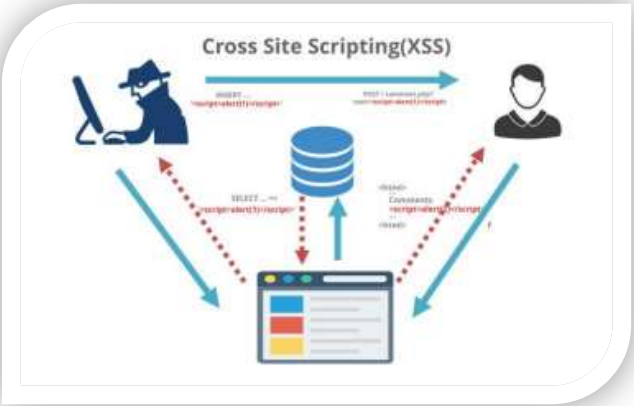
3. Sisipkan Kode Berbahaya: Penyerang menyisipkan kode SQL berbahaya ke dalam input yang diharapkan oleh aplikasi. Kode ini sering kali dimasukkan dalam bentuk string atau parameter yang diharapkan oleh query SQL.
4. Eksekusi Kode SQL Berbahaya: Ketika aplikasi tidak memvalidasi atau melindungi input dengan benar, perintah SQL yang berbahaya yang disisipkan oleh penyerang dieksekusi oleh database. Ini bisa menyebabkan pengeksekusian perintah yang tidak sah, pemilihan atau pemfilteran data yang tidak sesuai, atau bahkan modifikasi atau penghapusan data yang ada.
5. Eksploitasi Hasil: Penyerang menggunakan hasil eksekusi query SQL yang berbahaya untuk mencuri, memanipulasi, atau mengungkapkan data sensitif dari database, seperti informasi pengguna, informasi keuangan, atau data penting lainnya. Data ini kemudian dapat digunakan untuk tujuan jahat, seperti pencurian identitas, penipuan, atau pelanggaran privasi.

8.6.2 Serangan *Cross-Site Scripting* (XSS)

Serangan XSS terjadi ketika penyerang menyisipkan skrip berbahaya ke dalam halaman web yang kemudian dijalankan oleh browser pengguna. Serangan ini memungkinkan penyerang mencuri informasi pengguna atau mengendalikan sesi pengguna. Serangan *Cross-Site Scripting* (XSS) adalah serangan yang memanfaatkan celah keamanan pada aplikasi web yang memungkinkan penyerang menyisipkan skrip berbahaya (*script*) ke dalam halaman web yang dilihat oleh pengguna lain. Skrip ini kemudian dieksekusi oleh browser pengguna, tanpa pemvalidasian atau filtering yang memadai.

Terdapat tiga jenis serangan XSS utama yaitu:

1. *Reflected* XSS: Serangan ini terjadi ketika skrip berbahaya disisipkan ke dalam parameter URL atau form input yang kemudian ditampilkan dalam halaman web. Ketika pengguna mengakses halaman tersebut, skrip tersebut dieksekusi oleh browser pengguna.
2. *Stored* XSS: Serangan ini terjadi ketika skrip berbahaya disisipkan ke dalam database atau penyimpanan yang terkait dengan aplikasi web, seperti kotak komentar atau profil pengguna. Skrip tersebut kemudian dieksekusi ketika halaman yang mengandung skrip tersebut ditampilkan kepada pengguna lain.
3. DOM-*based* XSS: Serangan ini terjadi ketika skrip berbahaya memanipulasi struktur Dokumen Objek Model (DOM) pada sisi klien. Skrip tersebut memanipulasi elemen-elemen pada halaman web secara langsung melalui pemrosesan JavaScript di dalam browser pengguna. (Putra *et al.*, 2021)



Gambar 8.14. Cara Kerja Seranggan XSS
Sumber: https://www.jsisfotek.org/

Dampak dari serangan XSS dapat bervariasi, termasuk mencuri data pengguna, menyebarkan malware, melakukan phishing, merusak reputasi aplikasi atau situs web, dan mempengaruhi pengalaman pengguna secara keseluruhan

Berikut adalah langkah-langkah umum yang terjadi dalam serangan XSS:

1. Identifikasi Titik Rentan: Penyerang mencari celah keamanan pada aplikasi web yang memungkinkan mereka menyisipkan skrip berbahaya. Hal ini bisa terjadi jika aplikasi tidak memvalidasi atau menyaring input pengguna dengan benar sebelum menampilkan atau menyimpannya.
2. Sisipkan Skrip Berbahaya: Penyerang menyisipkan skrip berbahaya dalam bentuk kode JavaScript atau HTML ke dalam input yang diterima oleh aplikasi web. Ini bisa dilakukan melalui form input, parameter URL, kotak komentar, atau fitur lain yang menerima input pengguna.
3. Penyisipan Skrip ke dalam Halaman Web: Aplikasi web tidak memvalidasi atau memfilter input pengguna dengan benar sebelum menampilkannya dalam halaman web. Sebagai hasilnya, skrip berbahaya yang disisipkan oleh penyerang ditampilkan kepada pengguna lain sebagai bagian dari halaman web.
4. Eksekusi Skrip oleh Browser Pengguna: Ketika halaman web yang mengandung skrip berbahaya ditampilkan oleh browser pengguna, skrip tersebut dieksekusi secara otomatis oleh browser. Ini dapat mengakibatkan berbagai dampak, seperti mencuri informasi pengguna, melakukan aksi yang tidak diinginkan, atau memodifikasi tampilan halaman web.

Salah satu kasus terkenal yang melibatkan serangan XSS adalah serangan XSS pada situs web sosial terkenal, Twitter, pada

tahun 2010. Serangan tersebut dilakukan oleh seorang peneliti keamanan bernama "Mansour" yang menemukan celah keamanan pada fitur TweetDeck, sebuah aplikasi manajemen dan monitoring Twitter. Dalam serangan tersebut, Mansour menyisipkan skrip berbahaya ke dalam kolom pesan yang memungkinkan pengguna memasukkan teks dalam format HTML. Skrip berbahaya tersebut kemudian dieksekusi oleh browser pengguna yang membuka tweet tersebut. Serangan ini memungkinkan Mansour mengirim tweet yang mengandung skrip XSS kepada pengikutnya, sehingga skrip tersebut akan dieksekusi ketika pengikut membuka tweet tersebut di Twitter atau melalui aplikasi TweetDeck.

Dampaknya adalah serangan XSS ini memungkinkan penyerang untuk mencuri token otentikasi Twitter pengguna, mengirim tweet dari akun pengguna yang terkena, dan bahkan memanipulasi akun pengguna yang terhubung dengan TweetDeck. Twitter segera mengambil tindakan untuk menutup celah keamanan dan memperbaiki kerentanan yang ditemukan.

8.6.3 Serangan *Cross-Site Request Forgery* (CSRF)

Serangan CSRF melibatkan eksekusi tindakan tidak diinginkan pada website pengguna tanpa persetujuan mereka. Penyerang memanfaatkan kepercayaan yang ada antara pengguna dan website untuk melakukan tindakan yang tidak diinginkan, seperti mengubah pengaturan atau melakukan transaksi.

Proses serangan CSRF biasanya melibatkan langkah-langkah berikut:

1. Penyerang mempersiapkan atau memanipulasi halaman web yang mengandung tindakan yang akan dilakukan oleh pengguna yang diautentikasi. Hal ini bisa berupa tautan, gambar, atau bentuk lain yang akan memicu tindakan pada aplikasi web target.
2. Penyerang mengirimkan atau menyebarluaskan halaman web tersebut ke pengguna yang diautentikasi. Hal ini dapat

dilakukan melalui email, media sosial, atau metode lain untuk mengelabui pengguna agar membuka halaman tersebut.

3. Ketika pengguna yang diautentikasi membuka halaman tersebut, permintaan otomatis dikirimkan oleh browser pengguna ke aplikasi web target tanpa pengetahuan atau persetujuan pengguna. Permintaan tersebut bisa berupa operasi yang merusak, seperti mengubah pengaturan akun, mengirim pesan, atau melakukan tindakan berbahaya lainnya.

Gambar 8.15. Cara Kerja Serangan Cross-Site Request Forgery (CSRF)
Sumber: https://www.atatus.com/

Serangan *Cross-Site Request Forgery* (CSRF) dapat memiliki dampak yang berpotensi merugikan bagi pengguna dan aplikasi web target. Beberapa dampak umum dari serangan CSRF adalah:

1. Aksi yang Tidak Diinginkan: Serangan CSRF memungkinkan penyerang untuk memaksa pengguna yang diautentikasi melakukan tindakan yang tidak diinginkan pada aplikasi web target tanpa sepengetahuan atau persetujuan mereka. Hal ini bisa termasuk mengubah pengaturan akun, mengirim pesan, memposting konten yang tidak diinginkan, atau melakukan tindakan berbahaya lainnya.
2. Manipulasi Data Pengguna: Dalam serangan CSRF, penyerang dapat memanipulasi data pengguna dengan mengirim permintaan palsu. Misalnya, penyerang dapat mengubah alamat pengiriman atau informasi keuangan pada profil pengguna, merubah preferensi atau pengaturan pengguna, atau menghapus atau mengubah data yang sensitif.
3. Kerugian Finansial: Serangan CSRF dapat digunakan untuk melakukan tindakan yang dapat menyebabkan kerugian finansial bagi pengguna atau aplikasi web target. Misalnya, penyerang dapat memaksa pengguna untuk melakukan transaksi keuangan yang tidak diinginkan atau mengubah informasi pembayaran.
4. Kompromi Akun Pengguna: Jika serangan CSRF berhasil, penyerang dapat mengakibatkan kompromi akun pengguna. Penyerang dapat mengubah kata sandi, alamat email, atau informasi akun lainnya, memperoleh akses ke informasi pribadi pengguna, atau menggunakan akun pengguna untuk tujuan jahat lainnya.
5. Penyebaran Malware atau Phishing: Dalam beberapa kasus, serangan CSRF dapat digunakan untuk memanipulasi pengguna agar mengunduh atau menjalankan malware,

atau mengalihkan mereka ke situs phishing yang meniru tampilan aplikasi web target. Ini dapat mengakibatkan pencurian informasi sensitif atau kerugian keuangan.

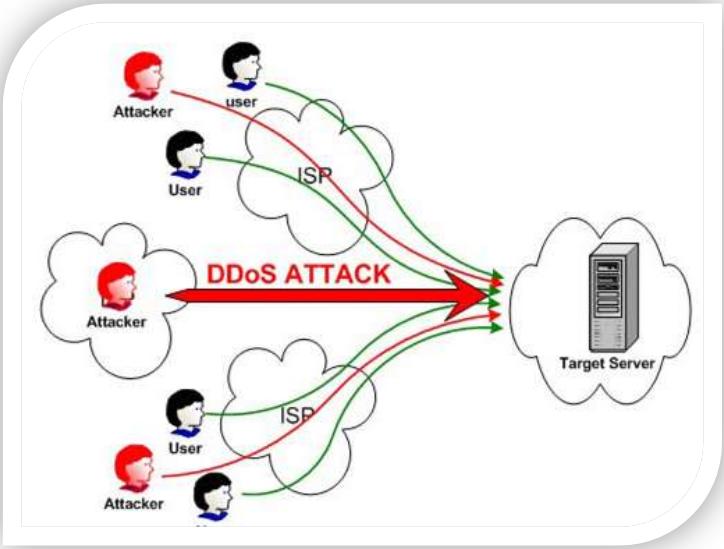
6. Kerusakan Reputasi: Jika serangan CSRF terjadi pada aplikasi web yang dikelola dengan buruk atau populer, hal ini dapat merusak reputasi aplikasi web dan mempengaruhi kepercayaan pengguna. Serangan terhadap data pengguna atau aksi yang tidak diinginkan dapat menyebabkan kehilangan pengguna atau merusak citra aplikasi web tersebut.

Salah satu kasus serangan *Cross-Site Request Forgery* (CSRF) yang terjadi pada tahun 2019 adalah serangan terhadap platform jejaring sosial Instagram. Pada tahun itu, terungkap bahwa terdapat kerentanan CSRF yang memungkinkan penyerang memposting konten atau mengubah pengaturan akun pengguna tanpa persetujuan mereka. Pada serangan ini, penyerang dapat memanfaatkan tautan atau halaman web yang mengandung kode CSRF yang dirancang untuk memicu tindakan tertentu pada akun Instagram pengguna yang telah diautentikasi. Ketika pengguna mengklik tautan atau mengunjungi halaman tersebut, permintaan palsu akan secara otomatis dikirimkan melalui browser pengguna, yang dapat mengubah konten atau pengaturan akun pengguna tanpa sepengetahuan mereka. Serangan ini dapat menyebabkan pengguna kehilangan kendali atas akun mereka, penyebaran konten yang tidak diinginkan atau berbahaya, atau perubahan yang merugikan terhadap profil dan preferensi mereka. (Quispe, 2023)

Setelah kerentanan ini ditemukan, Instagram dan tim keamanan mereka mengambil tindakan untuk memperbaiki kerentanan dan meningkatkan keamanan platform mereka. Mereka melakukan perbaikan pada implementasi CSRF dan melaksanakan langkah-langkah pencegahan tambahan untuk melindungi pengguna dari serangan semacam itu.

8.6.4 Serangan DDoS (*Distributed Denial of Service*)

Serangan DDoS bertujuan untuk mengganggu atau melumpuhkan layanan dengan mengirimkan lalu lintas yang sangat tinggi ke server atau jaringan. Serangan DDoS melibatkan penggunaan banyak mesin yang dikompromikan atau sumber daya yang didistribusikan untuk menghancurkan infrastruktur target. Serangan DDoS (*Distributed Denial of Service*) adalah serangan yang dilakukan dengan cara membanjiri sebuah sistem atau jaringan dengan lalu lintas internet yang sangat tinggi. Tujuan dari serangan ini adalah untuk membuat sistem atau jaringan tersebut tidak dapat beroperasi secara normal dan mengakibatkan layanan menjadi tidak tersedia bagi pengguna yang sah.



Gambar 8.16. Cara Kerja Serangan DDoS (*Distributed Denial of Service*)
Sumber: https://www.berita2bahasa.com/

Serangan DDoS dilakukan dengan menggerakkan banyak perangkat yang terinfeksi malware atau botnet untuk mengirimkan sejumlah besar permintaan atau paket data ke target yang dituju secara bersamaan. Dalam serangan DDoS, para penyerang seringkali menggunakan jaringan yang terdistribusi secara geografis, sehingga sulit untuk mengidentifikasi dan memblokir serangan dari sumber yang spesifik.

Dampak dari serangan DDoS dapat beragam, termasuk:

1. Penurunan kinerja dan kecepatan layanan: Serangan DDoS yang berhasil dapat menyebabkan penurunan kinerja sistem atau jaringan target. Hal ini dapat mengakibatkan penurunan kecepatan akses, waktu respons yang lambat, atau bahkan kegagalan total layanan.
2. Gangguan operasional: Serangan DDoS yang intens dapat membuat sistem atau jaringan menjadi tidak berfungsi sama sekali, menghentikan layanan yang terkait dan mengakibatkan kerugian finansial serta kerugian reputasi bagi organisasi yang menjadi korban.
3. Gangguan bisnis: Organisasi yang menjadi target serangan DDoS dapat mengalami dampak finansial yang signifikan akibat layanan yang tidak tersedia atau terganggu. Bisnis dapat kehilangan pelanggan, reputasi yang tercemar, dan dampak jangka panjang pada operasi mereka.
4. Pengalihan sumber daya: Selama serangan DDoS, sumber daya sistem dan jaringan yang terbatas akan digunakan untuk menangani lalu lintas yang tidak sah. Hal ini dapat mengalihkan perhatian dan sumber daya dari tugas yang sebenarnya, seperti pemrosesan permintaan pengguna yang sah.

Berikut ini adalah langkah-langkah umum yang terlibat dalam cara kerja serangan DDoS:

1. Penyusunan Botnet: Penyerang biasanya mengumpulkan sejumlah besar perangkat yang terinfeksi malware atau botnet. Botnet terdiri dari komputer, server, atau perangkat IoT yang dikendalikan oleh penyerang secara jarak jauh tanpa pengetahuan pemiliknya.
2. Pengendalian Botnet: Penyerang mengendalikan botnet untuk mengirimkan lalu lintas internet yang tinggi ke target yang dituju. Mereka dapat menggunakan perintah dan kontrol jarak jauh (C&C) untuk mengoordinasikan serangan.
3. Identifikasi Target: Penyerang memilih target yang ingin diserang, seperti situs web, server, atau jaringan khusus. Target ini mungkin merupakan entitas yang diinginkan oleh penyerang, atau mereka bisa menjadi korban serangan acak.
4. Inisiasi Serangan: Botnet mulai mengirimkan lalu lintas ke target dengan intensitas tinggi. Serangan dapat menggunakan berbagai metode, seperti HTTP flood, ICMP flood, UDP flood, SYN flood, atau kombinasi dari beberapa metode tersebut.
5. Pembanjiran Sumber Daya: Lalu lintas yang tinggi dari botnet membebani sumber daya sistem atau jaringan target. Ini dapat meliputi bandwidth, prosesor, memori, atau sumber daya jaringan lainnya. Seiring dengan bertambahnya lalu lintas, target mengalami penurunan kinerja atau bahkan kegagalan total dalam menyediakan layanan kepada pengguna yang sah.
6. Kesulitan Deteksi: Serangan DDoS seringkali menggunakan sumber daya yang terdistribusi secara geografis, sehingga sulit untuk mengidentifikasi sumber serangan secara spesifik. Ini membuat tugas memblokir serangan atau

mengambil tindakan melawan penyerang menjadi lebih rumit.

Cara kerja serangan DDoS bergantung pada penggunaan botnet dan kemampuannya untuk menghasilkan lalu lintas yang tinggi. Penyerang berharap bahwa target tidak dapat menangani beban lalu lintas yang besar dan mengalami penurunan kinerja atau kegagalan, sehingga menyebabkan layanan menjadi tidak tersedia bagi pengguna yang sah. (Hudaya & Primananda, 2023)

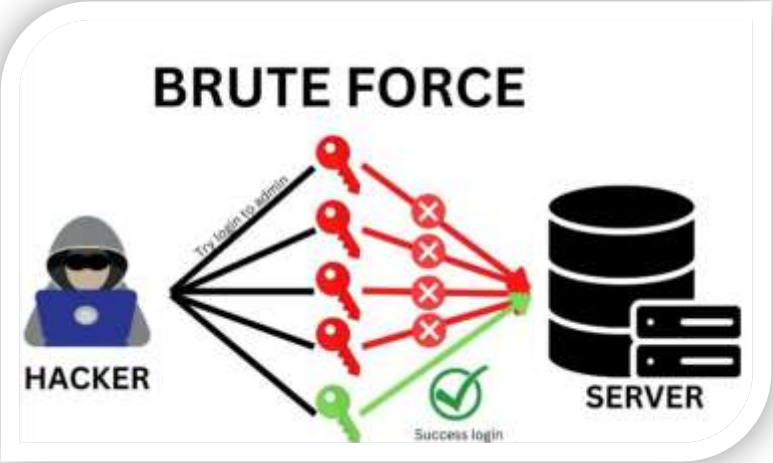
Salah satu kasus yang terjadi akibat serangan DDoS pada tahun 2019 adalah serangan DDoS terhadap layanan Cloudflare. Pada bulan Juni 2019, layanan Cloudflare, yang merupakan salah satu penyedia perlindungan DDoS terbesar di dunia, mengalami serangan DDoS massal yang menyebabkan gangguan pada layanan mereka. Serangan DDoS tersebut diklaim sebagai serangan terbesar yang pernah terjadi pada saat itu, dengan lalu lintas mencapai 18 juta permintaan per detik. Akibat serangan tersebut, beberapa situs web yang menggunakan layanan Cloudflare mengalami penurunan kinerja atau bahkan kegagalan total.

Serangan DDoS terhadap Cloudflare ini menunjukkan bahwa bahkan penyedia perlindungan DDoS yang besar dan kuat pun dapat menjadi target serangan tersebut. Hal ini juga menggarisbawahi pentingnya perlindungan dan mitigasi yang kuat terhadap serangan DDoS, bahkan bagi perusahaan yang telah berinvestasi dalam solusi keamanan jaringan.

8.6.5 Serangan Brute Force

Serangan *Brute force* melibatkan upaya berulang untuk menebak kombinasi username dan password dengan harapan mendapatkan akses tidak sah ke sistem atau akun pengguna. Penyerang menggunakan program otomatis untuk mencoba ribuan atau jutaan kombinasi password secara berurutan. Cara kerja serangan Brute Force adalah dengan menggunakan program

atau skrip otomatis yang secara berulang mencoba kombinasi kata sandi secara berurutan hingga menemukan yang benar. Program ini bisa mencoba kata sandi dengan menggabungkan huruf, angka, dan karakter khusus dalam berbagai pola dan panjang.



Gambar 8.17. Serangan Brute Force
Sumber: https://taufikcrisnawan.dev/

Serangan Brute Force dapat menjadi ancaman serius jika kata sandi yang digunakan lemah atau mudah ditebak. Dalam banyak kasus, serangan ini memanfaatkan ketidakseimbangan antara kekuatan kata sandi yang lemah dengan kemampuan komputasi yang semakin meningkat dari komputer modern dan sumber daya komputasi yang tersedia.
Dampak dari serangan Brute Force dapat meliputi:

1. Kompromi Akun: Jika serangan Brute Force berhasil, penyerang dapat mendapatkan akses tidak sah ke akun seseorang. Ini dapat digunakan untuk mencuri informasi

pribadi, mengubah data, atau melancarkan serangan lebih lanjut.
2. Pengungkapan Data Sensitif: Jika serangan Brute Force berhasil pada sistem atau layanan yang menyimpan data sensitif, seperti basis data pelanggan, informasi keuangan, atau rahasia bisnis, maka data tersebut dapat diungkapkan atau digunakan secara tidak sah.
3. Kegagalan Layanan: Serangan Brute Force yang terjadi pada sistem autentikasi atau keamanan yang lemah dapat menyebabkan kegagalan layanan atau penurunan kinerja sistem yang signifikan.

Cara kerja serangan Brute Force adalah dengan mencoba semua kemungkinan kombinasi kata sandi secara berurutan hingga menemukan kata sandi yang benar. Berikut ini adalah langkah-langkah umum dalam cara kerja serangan Brute Force: (Mulyanto *et al.,* 2022)

1. Identifikasi Target: Penyerang harus mengidentifikasi target yang ingin diserang, seperti akun pengguna, sistem autentikasi, atau layanan tertentu.
2. Membangun Daftar Kata Sandi: Penyerang perlu membangun daftar kata sandi yang akan dicoba secara berurutan. Daftar ini bisa berupa kombinasi huruf, angka, dan karakter khusus dengan panjang tertentu. Semakin panjang daftar dan semakin kompleks kombinasi kata sandi, semakin lama serangan Brute Force akan memakan waktu.
3. Mencoba Kata Sandi: Penyerang menggunakan program atau skrip otomatis untuk mencoba satu per satu kombinasi kata sandi dari daftar yang telah disusun. Setiap kata sandi yang dicoba akan dikirimkan ke target untuk mencoba masuk atau mendapatkan akses.

4. Verifikasi Keberhasilan: Setelah mencoba satu kata sandi, penyerang akan memverifikasi apakah kata sandi tersebut berhasil dalam mendapatkan akses atau tidak. Jika kata sandi berhasil, penyerang mendapatkan akses tidak sah ke akun atau sistem target. Jika kata sandi gagal, penyerang akan mencoba kata sandi berikutnya dalam daftar.
5. Proses Berulang: Penyerang akan terus mencoba semua kombinasi kata sandi dalam daftar sampai menemukan kata sandi yang benar atau hingga semua kemungkinan kata sandi telah dicoba.

Cara kerja serangan Brute Force didasarkan pada logika sederhana dan kekuatan komputasi yang tinggi. Semakin panjang dan kompleks kata sandi yang digunakan, semakin lama waktu yang dibutuhkan untuk menemukan kata sandi yang benar. Namun, dengan kemajuan teknologi komputasi, penyerang dapat menggunakan sumber daya komputasi yang besar, seperti botnet atau komputer terdistribusi, untuk mempercepat proses serangan Brute Force.

Beberapa kasus serangan Brute Force yang signifikan di berbagai sektor dan platform. Berikut ini adalah beberapa kasus terkenal yang terjadi selama tahun 2020:

1. Serangan *Brute Force* pada Akun Microsoft: Pada September 2020, Microsoft melaporkan bahwa sekitar 1% dari akun pengguna mereka mengalami serangan Brute Force. Serangan ini dilakukan dengan mencoba kombinasi kata sandi yang berbeda secara berulang pada akun pengguna Microsoft.
2. Serangan *Brute Force* pada *Platform eCommerce*: Beberapa platform eCommerce mengalami serangan Brute Force pada tahun 2020. Serangan ini bertujuan untuk mencoba mendapatkan akses ke akun pelanggan atau mengakses

informasi kartu kredit yang tersimpan pada platform tersebut.

3. Serangan *Brute Force* pada Sistem CMS: Serangan *Brute Force* juga sering terjadi pada *sistem Content Management System* (CMS) seperti WordPress atau Joomla. Penyerang menggunakan skrip otomatis untuk mencoba kombinasi kata sandi pada halaman login CMS, dengan tujuan mendapatkan akses administrator atau mengubah konten situs web.
4. Serangan Brute Force pada Router dan Perangkat IoT: Serangan Brute Force juga ditargetkan pada router dan perangkat *Internet of Things* (IoT). Penyerang mencoba kombinasi kata sandi default atau lemah pada perangkat tersebut untuk mendapatkan akses dan mengambil alih kontrol perangkat.

8.6.6 Serangan *Man-in-the-Middle* (MitM)

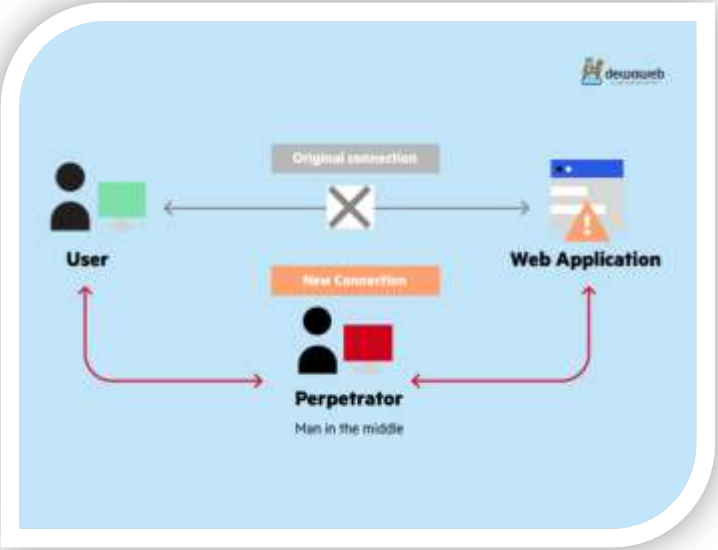
Serangan MitM terjadi ketika penyerang mencampuri komunikasi antara dua pihak yang berinteraksi, seperti antara pengguna dan website. Penyerang dapat memata-matai, mengubah, atau mencuri informasi yang dikirimkan antara pihak-pihak yang berkomunikasi.

Berikut adalah langkah-langkah umum yang terjadi dalam serangan *Man-in-the-Middle*:

1. Pemantauan Komunikasi: Penyerang memantau komunikasi yang terjadi antara dua pihak yang sedang berinteraksi. Ini bisa dilakukan dengan menggunakan alat pengawasan jaringan, seperti sniffer atau perangkat yang dipasang di tengah jalur komunikasi.
2. Pemutusan Koneksi: Setelah penyerang memantau komunikasi, mereka dapat memutuskan koneksi antara dua pihak yang berkomunikasi, sehingga mereka dapat

menyisipkan diri di tengah-tengah dan mengendalikan aliran data.

3. Penyusupan Data: Setelah mendapatkan kendali atas komunikasi, penyerang dapat menyusupkan, mengubah, atau mencuri data yang dikirimkan antara dua pihak. Ini bisa mencakup pencurian informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi.
4. Pemalsuan Identitas: Dalam serangan MitM, penyerang juga dapat memalsukan identitas mereka sebagai pihak yang asli. Dengan demikian, mereka dapat membuat kedua pihak berpikir bahwa mereka sedang berkomunikasi langsung dengan pihak yang sebenarnya, sementara penyerang memantau dan memanipulasi semua informasi yang melewati mereka.



Gambar 8.18. Cara Kerja Attacker Menggunakan Serangan *Man-in-the-Middle* (MitM). Sumber: https://www.dewaweb.com/

Dampak serangan Man-in-the-Middle dapat sangat serius, terutama jika data sensitif atau informasi rahasia terlibat. Penyerang dapat mencuri informasi pribadi, melakukan pencurian identitas, mengakses akun pengguna, atau bahkan memanipulasi transaksi atau pesan yang dikirimkan antara pihak yang berkomunikasi.

Ada beberapa kasus terkenal serangan *Man-in-the-Middle* (MitM) yang terjadi di masa lalu. Berikut ini adalah beberapa contoh:

1. Serangan SSLstrip: Pada tahun 2009, seorang peneliti keamanan bernama Moxie Marlinspike mengungkapkan serangan SSLstrip yang memanfaatkan kelemahan dalam protokol HTTPS. Serangan ini dapat merubah lalu lintas HTTPS menjadi HTTP, sehingga penyerang dapat memantau dan mengakses data yang seharusnya terenkripsi.
2. Serangan MITM pada Jaringan Wi-Fi Publik: Jaringan Wi-Fi publik yang tidak aman menjadi target yang umum bagi serangan MitM. Penyerang dapat membuat jaringan Wi-Fi palsu dengan nama yang mirip dengan jaringan asli atau menggunakan teknik lainnya untuk menyusup ke dalam komunikasi antara pengguna dan titik akses Wi-Fi. Dengan demikian, mereka dapat mencuri informasi pribadi pengguna yang dikirim melalui jaringan.
3. Serangan MITM pada Aplikasi Perbankan Online: Beberapa kasus serangan MitM juga terjadi pada aplikasi perbankan online. Penyerang mencoba memanipulasi komunikasi antara pengguna dan aplikasi perbankan, sehingga mereka dapat mencuri kredensial login atau melakukan transaksi keuangan yang tidak sah.
4. Serangan MITM pada Protokol VoIP: Protokol *Voice over Internet Protocol* (VoIP) juga rentan terhadap serangan MitM. Penyerang dapat memanipulasi atau menyadap

komunikasi suara yang terjadi melalui protokol ini, sehingga mereka dapat mendengarkan percakapan atau melakukan rekaman yang tidak sah. (Pangestu & Liza, 2022)

8.6.7 Serangan Pharming

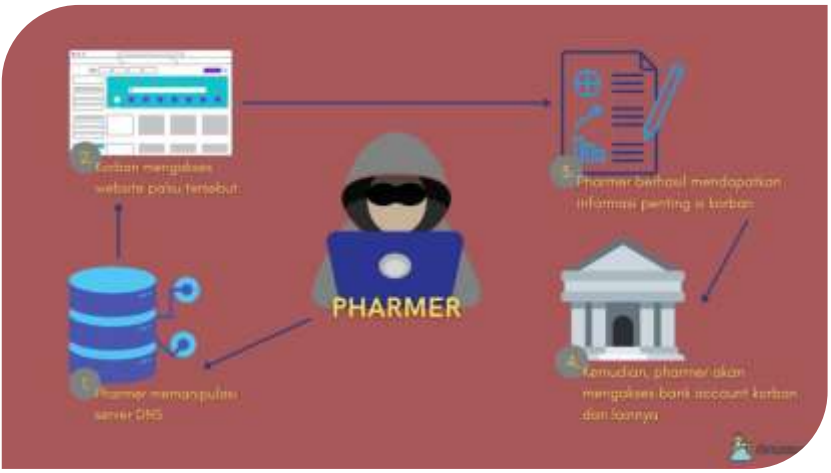
Serangan Pharming melibatkan pengalihan lalu lintas pengguna ke situs web palsu atau mencuri informasi pengguna dengan mengubah pengaturan DNS (*Domain Name System*) atau mengelabui pengguna untuk mengunjungi situs web palsu melalui manipulasi URL.Serangan Pharming bekerja dengan cara memanipulasi proses resolusi DNS (*Domain Name System*) untuk mengarahkan lalu lintas pengguna ke situs web palsu atau tidak sah. Berikut adalah langkah-langkah umum yang terjadi dalam serangan Pharming:

1. Pengalihan DNS:
    a. Penyerang memanipulasi server DNS atau perangkat yang bertindak sebagai resolver DNS.
    b. Mereka mengubah entri DNS yang terkait dengan nama domain asli (misalnya, www.bank.com) menjadi alamat IP situs web palsu yang dikendalikan oleh penyerang.
2. Cache Poisoning:
    a. Penyerang menggunakan teknik cache poisoning untuk menyebabkan server DNS menyimpan informasi palsu dalam cache-nya.
    b. Dengan cara ini, ketika pengguna mencoba mengakses situs web yang sebenarnya, resolver DNS akan mengambil data palsu dari cache dan mengarahkan pengguna ke situs web palsu.
3. Pembajakan Perangkat Lunak:
    a. Penyerang menginfeksi perangkat pengguna dengan perangkat lunak berbahaya atau malware.

b. Malware ini memodifikasi pengaturan DNS pada perangkat, baik melalui perubahan konfigurasi sistem operasi atau melalui aplikasi tertentu yang terinstal pada perangkat.
c. Akibatnya, saat pengguna mencoba mengakses situs web yang sebenarnya, perangkat akan mengarahkan mereka ke situs web palsu yang dikendalikan oleh penyerang.

4. Pembajakan Jaringan:
   a. Penyerang memanipulasi jaringan, misalnya dengan menggunakan serangan *man-in-the-middle* (MitM) atau membuat hotspot Wi-Fi palsu.
   b. Ketika pengguna terhubung ke jaringan yang telah dibajak, semua permintaan DNS yang mereka lakukan akan diarahkan ke server DNS yang dikendalikan oleh penyerang. Ini memungkinkan penyerang untuk mengarahkan pengguna ke situs web palsu.

Cara kerja serangan Pharming dapat sangat merugikan, karena pengguna dapat diarahkan ke situs web palsu yang dirancang untuk mencuri informasi pribadi mereka, seperti nama pengguna, kata sandi, atau rincian keuangan. Penyerang kemudian dapat menggunakan informasi ini untuk kegiatan ilegal, seperti pencurian identitas atau penipuan. (Sari *et al.*, 2022)



Gambar 8.19. Langkah-langkah Serangan Pharming
Sumber: https://www.dewaweb.com/

Berikut adalah beberapa kasus yang terkenal terkait serangan Pharming:

1. Kasus *Sony PlayStation Network* (2011): Pada tahun 2011, serangan Pharming terjadi pada jaringan PlayStation Network milik Sony. Serangan tersebut menyebabkan lebih dari 70 juta akun pengguna PlayStation Network terkena dampak. Para penyerang berhasil memanipulasi pengaturan DNS dan mengarahkan pengguna ke situs web palsu yang meniru tampilan asli PlayStation Network. Serangan ini mengakibatkan pencurian informasi pribadi pengguna, termasuk nama, alamat, dan informasi kartu kredit.
2. Kasus PayPal (2005): Pada tahun 2005, serangan Pharming terjadi pada PayPal, platform pembayaran online yang populer. Serangan tersebut menggunakan teknik *cache poisoning* dan mengarahkan pengguna ke situs web palsu yang meniru tampilan PayPal asli. Penyerang mencoba mendapatkan informasi login dan rincian keuangan

pengguna. Kasus ini menyebabkan kekhawatiran tentang keamanan transaksi online dan menekankan pentingnya perlindungan terhadap serangan Pharming.

3. Kasus *Bank of India* (2016): Pada tahun 2016, serangan Pharming menargetkan Bank of India. Penyerang menggunakan teknik DNS spoofing untuk memanipulasi pengaturan DNS dan mengarahkan pengguna ke situs web palsu yang meniru tampilan Bank of India. Tujuan serangan ini adalah untuk mencuri informasi login dan keuangan pengguna. Kasus ini menyoroti kerentanan yang ada dalam infrastruktur perbankan dan pentingnya langkah-langkah keamanan yang kuat.

8.6.8 Serangan File Inclusion

Serangan Serangan File Inclusion adalah serangan keamanan yang dapat mengancam aplikasi web dengan cara memanipulasi mekanisme penyertaan file yang ada. Dalam serangan ini, penyerang berhasil memasukkan atau menyisipkan file yang tidak aman atau tidak sah ke dalam halaman web yang ditampilkan kepada pengguna. Serangan File Inclusion terjadi ketika aplikasi web tidak memvalidasi atau tidak memproses dengan benar parameter input yang diterima, yang memungkinkan penyerang untuk mengakses file atau sumber daya sistem yang tidak seharusnya diakses.

Terdapat dua jenis utama serangan File Inclusion yang umum terjadi: *Local File Inclusion* (LFI) dan *Remote File Inclusion* (RFI). Mari kita bahas keduanya lebih rinci:

1. *Local File Inclusion* (LFI): Serangan LFI terjadi ketika penyerang berhasil menyisipkan file lokal yang ada pada server atau sistem yang menjalankan aplikasi web. Biasanya, aplikasi web menggunakan parameter untuk mengambil file lokal dan menyertakannya ke dalam halaman web yang ditampilkan. Namun, jika parameter

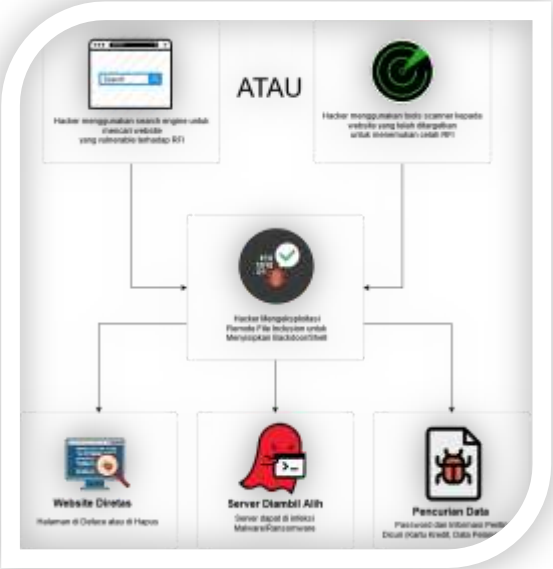
input tidak diverifikasi atau diproses dengan benar, penyerang dapat memanipulasinya dengan mengirimkan path file lokal yang diinginkan. Akibatnya, aplikasi web akan menyertakan file yang tidak seharusnya diakses oleh pengguna. Penyerang dapat memanfaatkan ini untuk mengakses file konfigurasi, kode sumber, atau bahkan data sensitif seperti file log yang berisi informasi rahasia.

2. *Remote File Inclusion* (RFI): Serangan RFI terjadi ketika penyerang berhasil menyisipkan file eksternal yang berada di server yang berbeda atau domain yang dikendalikan oleh penyerang. Serangan ini terjadi ketika aplikasi web mengizinkan penyertaan file eksternal tanpa melakukan validasi yang memadai. Penyerang dapat memanfaatkan ini dengan mengirimkan URL file eksternal yang diinginkan. Akibatnya, aplikasi web akan menyertakan file tersebut ke dalam halaman web yang ditampilkan kepada pengguna. Penyerang dapat menggunakan file ini untuk memasukkan kode jahat atau file yang memungkinkan mereka mengambil alih kendali atas server atau sistem yang terkena dampak.

Dampak dari serangan File Inclusion dapat sangat merugikan. Beberapa dampak yang mungkin terjadi adalah sebagai berikut:

1. Pengungkapan Informasi Sensitif: Serangan *File Inclusion* dapat mengakibatkan pengungkapan informasi sensitif yang seharusnya tidak dapat diakses oleh pengguna. Jika penyerang berhasil menyisipkan file yang mengandung informasi rahasia, seperti file konfigurasi atau file log, mereka dapat mengakses data tersebut. Hal ini dapat mengungkapkan rincian sistem, alamat IP, kredensial database, atau bahkan informasi pengguna yang dienkripsi.

2. Eksekusi Kode yang Tidak Sah: Jika penyerang berhasil menyisipkan kode jahat melalui serangan File Inclusion, mereka dapat menjalankan kode tersebut pada server atau sistem yang terkena dampak. Kode ini dapat digunakan untuk melakukan eksekusi perintah yang tidak sah, penyalahgunaan akses sistem.



Gambar 8.20. Ilustrasi Serangan File Inclusion
Sumber: https://www.ethic.ninja/

Terdapat beberapa kasus yang terkenal yang melibatkan serangan File Inclusion. Berikut adalah beberapa contohnya:

1. Kasus RFI pada MySpace (2005): Pada tahun 2005, serangan *Remote File Inclusion* (RFI) terjadi pada platform media sosial MySpace. Penyerang berhasil menyisipkan kode jahat ke dalam halaman profil pengguna dengan memanfaatkan celah RFI. Kode jahat ini kemudian

digunakan untuk mencuri informasi pengguna, termasuk kata sandi, dan menjalankan aksi yang tidak sah.

2. Kasus LFI pada bahan ajar UCLA (2006): Pada tahun 2006, *Universitas California, Los Angeles* (UCLA) menjadi target serangan *Local File Inclusion* (LFI). Penyerang berhasil memanipulasi parameter input pada sistem manajemen bahan ajar untuk mendapatkan akses ke file-file yang sensitif. Serangan ini mengungkapkan informasi penting tentang dosen dan mahasiswa.
3. Kasus RFI pada situs web Indosat (2012): Pada tahun 2012, situs web penyedia layanan telekomunikasi terbesar di Indonesia, yaitu Indosat, mengalami serangan RFI. Penyerang berhasil menyisipkan skrip jahat ke dalam halaman web Indosat dan menyebabkan pengalihan pengguna ke situs web palsu. Serangan ini mempengaruhi ribuan pengguna dan mencuri informasi pribadi mereka.
4. Kasus LFI pada situs web Yahoo! Voices (2012): Pada tahun 2012, serangan LFI terjadi pada situs web Yahoo! Voices (dahulu dikenal sebagai *Associated Content*). Penyerang memanfaatkan celah LFI untuk menyisipkan kode jahat ke dalam halaman web dan mengakses database pengguna. Serangan ini mengakibatkan informasi lebih dari 450.000 akun pengguna Yahoo! terekspos.
5. Kasus RFI pada situs web Bangladesh Bank (2016): Pada tahun 2016, serangan RFI dilakukan pada situs web Bank Bangladesh. Penyerang berhasil menyisipkan skrip jahat ke dalam halaman web bank yang tidak terlindungi dengan baik. Serangan ini memungkinkan penyerang untuk mencuri kredensial pengguna dan mencoba melakukan transfer dana yang signifikan.

8.6.9 Serangan Server Side Request Forgery (SSRF)

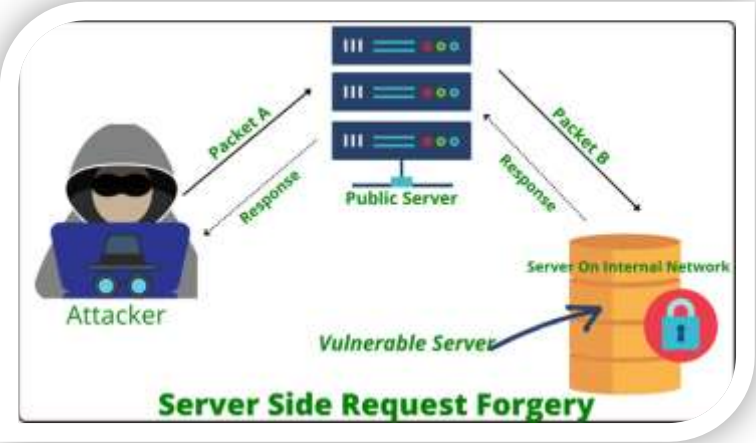
Serangan SSRF melibatkan penyerang mengirimkan permintaan dari server yang diserang ke sumber daya internal atau eksternal yang dapat diakses oleh server, termasuk server internal, file lokal, atau layanan cloud, yang kemudian dapat dieksploitasi. SSRF terjadi ketika penyerang berhasil memanipulasi input yang digunakan oleh server untuk membuat permintaan HTTP ke sumber daya yang tidak seharusnya dapat diakses olehnya. Penyerang memanfaatkan celah dalam aplikasi untuk menyusun permintaan yang berpotensi membocorkan informasi sensitif, mengeksploitasi sumber daya internal yang tidak diinginkan, atau melakukan serangan terhadap sistem lain di jaringan. (Zirwan, 2022)

Dampak: Serangan SSRF dapat memiliki dampak serius terhadap keamanan dan kerahasiaan aplikasi serta infrastruktur yang terkait. Berikut adalah beberapa dampak yang mungkin terjadi:

1. Akses ke Sumber Daya Internal: Penyerang dapat memanfaatkan SSRF untuk mengakses sumber daya internal seperti file sistem, database, server aplikasi, atau jaringan internal yang hanya seharusnya dapat diakses oleh server aplikasi. Ini dapat mengakibatkan pencurian data sensitif, perusakan atau manipulasi data, atau akses tidak sah ke sistem penting.
2. Eksposur Informasi Penting: Dalam serangan SSRF, penyerang dapat mengirim permintaan ke sumber daya yang berisi informasi rahasia seperti kredensial autentikasi, file konfigurasi, atau log sistem. Dengan mendapatkan akses ke informasi ini, penyerang dapat memperoleh wawasan tentang infrastruktur aplikasi dan mempersiapkan serangan lanjutan.
3. Penyalahgunaan Sumber Daya Eksternal: Dalam beberapa kasus, SSRF dapat digunakan oleh penyerang untuk

mengeksploitasi sumber daya eksternal yang sensitif atau tidak diinginkan. Misalnya, penyerang dapat memanfaatkan SSRF untuk meluncurkan serangan terhadap sistem lain, menjalankan layanan yang tidak seharusnya diakses, atau memindahkan data keluar dari jaringan.

4. Kerusakan Reputasi dan Keuangan: Serangan SSRF dapat menyebabkan kerugian finansial dan reputasi bagi organisasi yang menjadi korban. Kerugian finansial dapat terjadi akibat pencurian data pelanggan atau perusakan infrastruktur. Kerugian reputasi dapat muncul akibat pelanggaran privasi data pelanggan, kebocoran informasi sensitif, atau ketidakmampuan untuk menyediakan layanan yang aman dan terpercaya.



Gambar 8.21. Serangan *Server Side Request Forgery* (SSRF)
Sumber: https://www.geeksforgeeks.org/

Cara kerja serangan SSRF dapat dijelaskan dengan langkah-langkah berikut:

1. Identifikasi Celah: Penyerang mencari celah dalam aplikasi web yang memungkinkan mereka mengendalikan atau memanipulasi permintaan HTTP yang dibuat oleh server. Hal ini bisa terjadi karena validasi input yang lemah atau penggunaan input pengguna tanpa sanitasi yang memadai.
2. Memanipulasi Parameter: Setelah menemukan celah, penyerang akan memanipulasi parameter atau input yang digunakan oleh server untuk membuat permintaan HTTP. Penyerang akan mencoba mengganti URL atau mengubah parameter lain dalam permintaan untuk mengarahkannya ke sumber daya yang tidak seharusnya dapat diakses oleh server.
3. Mengeksploitasi Sumber Daya Internal: Dalam serangan SSRF, penyerang dapat mencoba mengarahkan permintaan ke sumber daya internal seperti file sistem, server aplikasi, database, atau jaringan lokal yang tidak seharusnya dapat diakses oleh server aplikasi. Dengan memanipulasi URL dan parameter, penyerang dapat mencoba memperoleh akses ke sumber daya ini.
4. Pencurian Informasi: Jika penyerang berhasil melakukan SSRF ke sumber daya internal yang sensitif, mereka dapat mencuri informasi rahasia seperti kredensial autentikasi, file konfigurasi, atau data sensitif lainnya. Informasi ini dapat digunakan untuk melancarkan serangan lanjutan atau diperjualbelikan di pasar gelap.
5. Serangan Terhadap Sistem Lain: Selain mengakses sumber daya internal, serangan SSRF juga dapat digunakan untuk menyerang sistem lain dalam jaringan. Penyerang dapat mengarahkan permintaan ke sistem lain dalam jaringan yang rentan atau memanipulasi layanan lain yang dapat

diakses oleh server aplikasi, mengakibatkan kerusakan atau pengambilalihan sistem tersebut.

6. Penggunaan Jaringan Botnet: Dalam beberapa kasus, penyerang dapat menggunakan SSRF untuk mengarahkan permintaan ke sumber daya eksternal yang tidak diinginkan, seperti jaringan botnet. Dengan memanipulasi URL dan parameter, penyerang dapat mengarahkan permintaan ke alamat IP yang terkait dengan jaringan botnet, yang dapat digunakan untuk meluncurkan serangan terhadap sistem lain atau melakukan tindakan jahat lainnya.

8.6.10 Serangan Clickjacking

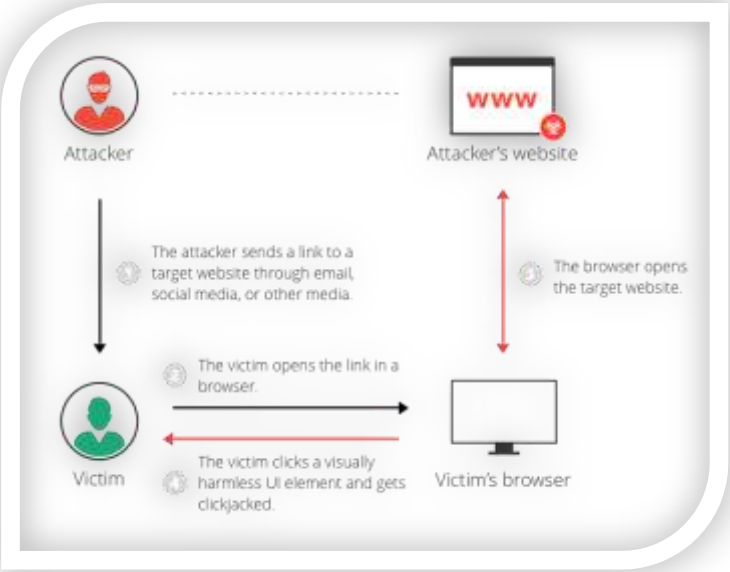
Serangan Clickjacking, juga dikenal sebagai UI redressing, adalah serangan yang dimaksudkan untuk menipu pengguna agar melakukan tindakan yang tidak disengaja atau tidak diinginkan pada sebuah situs web. Dalam serangan ini, penyerang mencoba memanipulasi tampilan atau presentasi halaman web untuk menipu pengguna agar mengklik elemen yang sebenarnya disembunyikan atau diposisikan secara jahat.

Cara kerja serangan Clickjacking adalah sebagai berikut:

1. Manipulasi Tampilan: Penyerang menciptakan halaman web yang terdiri dari lapisan yang tidak terlihat oleh pengguna. Lapisan ini dapat ditempatkan di atas konten yang sebenarnya atau di bawahnya.
2. Memanipulasi Element: Penyerang memanipulasi elemen dalam halaman web, seperti tombol, tautan, atau input form, dengan mengatur posisi dan ukuran mereka sehingga tidak terlihat atau disembunyikan dari pandangan pengguna.
3. Penyembunyian Aktivitas: Penyerang menggunakan CSS atau teknik lain untuk menyembunyikan elemen-elemen yang dimanipulasi dari pengguna, sehingga pengguna tidak

menyadari bahwa ada elemen yang sebenarnya tersembunyi di belakang elemen lain.

4. Pemindahan Klik: Ketika pengguna mengklik pada halaman web yang terlihat, mereka sebenarnya secara tidak sadar mengklik elemen yang dimanipulasi. Klik ini dapat mengakibatkan pengguna melakukan tindakan yang tidak diinginkan, seperti mengunggah file, memposting konten di media sosial, atau melakukan transaksi keuangan. (Hasibuan & Elhanafi, 2022).



Gambar 8.22. Cara Kerja Serangan Clickjacking
Sumber: https://www.imperva.com/

Dampak dari serangan Clickjacking dapat meliputi:

1. Pembajakan Akses: Serangan Clickjacking dapat memungkinkan penyerang mengambil alih akses pengguna ke akun online mereka, mengubah preferensi atau

pengaturan, atau bahkan melakukan tindakan yang berpotensi merugikan pengguna.
2. Pencurian Informasi: Dalam beberapa kasus, serangan Clickjacking dapat dimanfaatkan untuk mencuri informasi sensitif pengguna, seperti kata sandi, informasi kartu kredit, atau data pribadi lainnya.
3. Penyebaran Malware: Penyerang dapat menggunakan serangan Clickjacking sebagai cara untuk memperkenalkan malware ke sistem pengguna. Ketika pengguna mengklik elemen yang dimanipulasi, mereka mungkin secara tidak sadar mendownload atau menjalankan file berbahaya.

Berikut adalah beberapa contoh kasus serangan Clickjacking yang pernah terjadi:

1. Kasus "*Likejacking*" di Facebook: Penyerang memanipulasi tampilan halaman web yang menampilkan tombol "Like" di bawah konten menarik atau video yang menarik perhatian pengguna. Ketika pengguna mengklik di area tersebut, sebenarnya mereka secara tidak sadar memberikan suka pada postingan atau halaman tertentu tanpa disadari.
2. Kasus "UI *redressing*" pada aplikasi perbankan online: Penyerang menciptakan lapisan transparan di atas halaman web aplikasi perbankan online yang mengarahkan pengguna untuk memasukkan detail login mereka atau informasi sensitif lainnya ke dalam form palsu. Pengguna kemudian secara tidak sadar memberikan informasi pribadi mereka kepada penyerang.
3. Kasus "*Clickjacking* dalam iklan": Dalam beberapa kasus, iklan yang dipasang di situs web dapat dimanipulasi untuk menipu pengguna agar mengklik tautan atau tombol yang tidak diinginkan. Misalnya, penyerang dapat menyembunyikan tombol "*Close*" atau "*Skip*" dalam iklan dan memposisikannya di atas tombol "*Download*" yang

sebenarnya. Ketika pengguna mencoba menutup iklan, mereka sebenarnya mengklik tombol "Download" dan mengunduh file berbahaya.

4. Kasus "Clickjacking dalam video online": Penyerang dapat menggunakan teknik Clickjacking untuk mengarahkan pengguna untuk mengklik pada tautan atau tombol yang tersembunyi dalam video online yang mereka tonton. Ketika pengguna mengklik di area tersebut, mereka secara tidak sadar melakukan tindakan yang tidak diinginkan, seperti mengunduh file berbahaya atau mengirimkan informasi pribadi.

8.7 Langkah-langkah pencegahan serangan pada website

8.7.1 Serangan SQL Injection

Berikut adalah beberapa langkah-langkah pencegahan yang dapat diambil untuk mengurangi risiko serangan SQL Injection:

1. Validasi Input: Pastikan semua input yang diterima dari pengguna atau sumber eksternal lainnya divalidasi dengan benar sebelum digunakan dalam query SQL. Gunakan metode validasi seperti whitelist atau blacklist untuk memastikan bahwa input hanya mengandung karakter yang diizinkan dan menghindari karakter yang berpotensi berbahaya.
2. Parameterized Queries atau Prepared Statements: Gunakan teknik parameterized queries atau prepared statements dalam kode aplikasi untuk memisahkan perintah SQL dari data input. Ini memastikan bahwa data input diperlakukan sebagai nilai parameter terpisah, bukan sebagai bagian langsung dari perintah SQL. Dengan demikian, serangan SQL Injection dapat dicegah karena data input tidak akan dieksekusi sebagai perintah SQL.

3. Sanitisasi Data: Selain validasi input, pastikan juga untuk melakukan sanitasi data dengan menghapus atau menghindari karakter khusus, seperti tanda kutip (') atau karakter escape SQL, yang dapat dimanfaatkan dalam serangan SQL Injection. Gunakan teknik escape character atau fungsi sanitasi yang disediakan oleh bahasa pemrograman atau kerangka kerja yang digunakan.
4. Pembatasan Hak Akses Database: Berikan hak akses yang sesuai pada pengguna atau akun database yang digunakan oleh aplikasi. Pastikan hanya hak akses yang diperlukan untuk menjalankan perintah SQL yang relevan. Hal ini membantu membatasi kemampuan penyerang untuk memanipulasi atau mengambil data yang sensitif.
5. Patch dan Update Aplikasi: Pastikan aplikasi web Anda selalu diperbarui dengan versi terbaru dan terkini. Perusahaan perangkat lunak biasanya merilis pembaruan yang memperbaiki kerentanan keamanan, termasuk kerentanan terhadap serangan SQL Injection. Dengan memperbarui aplikasi secara teratur, Anda dapat mengurangi risiko serangan yang mungkin dieksploitasi.
6. Audit Keamanan Reguler: Lakukan audit keamanan secara berkala untuk mengidentifikasi kerentanan potensial dalam aplikasi web Anda. Gunakan alat keamanan yang tersedia untuk menguji keamanan aplikasi dan mendeteksi celah keamanan yang mungkin memungkinkan serangan SQL Injection.
7. Edukasi dan Kesadaran: Tingkatkan pengetahuan dan kesadaran tim pengembangan tentang serangan SQL Injection dan praktik keamanan aplikasi web yang baik. Pelatihan dan edukasi reguler akan membantu mengidentifikasi dan mengatasi kerentanan sejak awal dalam siklus pengembangan aplikasi.

Dengan mengadopsi langkah-langkah pencegahan ini, Anda dapat mengurangi risiko serangan SQL Injection dan menjaga keamanan aplikasi web Anda. Penting untuk selalu memprioritaskan keamanan dalam pengembangan dan pemeliharaan aplikasi web Anda.(Mushlih *et al.,* 2019)

8.7.2 Serangan *Cross-Site Scripting* (XSS)

Berikut adalah beberapa langkah-langkah pencegahan yang dapat diambil untuk mengurangi risiko serangan *Cross-Site Scripting* (XSS):

1. Validasi dan Sanitisasi Input: Pastikan semua input yang diterima dari pengguna atau sumber eksternal lainnya divalidasi dan disanitisasi dengan benar sebelum digunakan dalam tampilan halaman web. Gunakan metode validasi dan sanitasi yang sesuai untuk memastikan bahwa input hanya mengandung karakter yang diizinkan dan menghindari karakter yang berpotensi berbahaya.
2. Encoding Output: Saat menampilkan data pengguna atau input yang dikirim kembali ke halaman web, pastikan untuk melakukan encoding pada data tersebut. Encoding akan mengkonversi karakter-karakter yang berpotensi berbahaya menjadi representasi yang aman, sehingga tidak akan dieksekusi sebagai skrip oleh browser.
3. Filter dan Larang Karakter Khusus: Implementasikan filter yang memblokir atau melarang karakter-karakter khusus yang sering digunakan dalam serangan XSS, seperti tanda kutip (', "), tanda kurung sudut (<, >), atau karakter escape (). Dengan memfilter karakter-karakter ini, Anda dapat mengurangi kemungkinan terjadinya serangan XSS.
4. Implementasikan Content Security Policy (CSP): CSP adalah kebijakan keamanan yang dapat diterapkan di header HTTP untuk membatasi jenis sumber daya yang dapat dimuat oleh halaman web. Dengan menerapkan CSP, Anda

dapat membatasi pemrosesan skrip yang berasal dari sumber yang tidak dipercaya, mengurangi risiko serangan XSS.

5. Update Keamanan dan Pemeliharaan Reguler: Pastikan aplikasi web Anda selalu diperbarui dengan versi terbaru dan terkini. Perusahaan perangkat lunak seringkali merilis pembaruan keamanan yang memperbaiki kerentanan terhadap serangan XSS dan kerentanan keamanan lainnya. Dengan memperbarui aplikasi secara teratur, Anda dapat mengurangi risiko serangan yang mungkin dieksploitasi.
6. Penyuluhan dan Pelatihan Pengguna: Tingkatkan kesadaran pengguna tentang serangan XSS dan praktik keamanan yang baik. Berikan pelatihan kepada pengguna untuk mengenali tautan atau input yang mencurigakan, serta pentingnya tidak mempercayai atau mengklik tautan yang tidak diketahui atau mencurigakan.
7. Pengujian Keamanan Reguler: Lakukan pengujian keamanan reguler pada aplikasi web Anda, termasuk pengujian spesifik untuk mengidentifikasi kerentanan XSS. Gunakan alat pengujian keamanan yang tersedia atau melakukan pengujian manual untuk mengidentifikasi celah keamanan yang mungkin memungkinkan serangan XSS.(Putra et al., 2021)

8.7.3 Serangan *Cross-Site Request Forgery* (CSRF)

Berikut ini adalah beberapa langkah-langkah pencegahan yang dapat Anda terapkan untuk melindungi aplikasi web dari serangan *Cross-Site Request Forgery* (CSRF):

1. Implementasikan Token CSRF: Gunakan teknik token CSRF untuk melindungi aplikasi Anda. Setiap kali pengguna mengakses halaman yang melibatkan tindakan yang dapat mempengaruhi status server (seperti mengirim formulir atau melakukan perubahan data), berikan token CSRF yang

unik pada halaman tersebut. Token ini harus dikirimkan bersamaan dengan permintaan yang dilakukan oleh pengguna. Server kemudian dapat memeriksa token ini untuk memvalidasi permintaan dan memastikan bahwa permintaan berasal dari sumber yang sah.

2. Terapkan Double Submit Cookie: Metode ini melibatkan pengiriman token CSRF sebagai cookie HTTP dan dalam parameter permintaan yang dilakukan oleh pengguna. Saat permintaan dikirim, server akan memverifikasi kesesuaian token dalam cookie dan parameter. Jika keduanya cocok, permintaan dianggap valid.
3. Validasi Referer: Verifikasi referer HTTP header pada setiap permintaan yang diterima oleh server. Pastikan bahwa permintaan berasal dari sumber yang sah dan diijinkan untuk mengakses aplikasi.
4. Gunakan SameSite Cookies: Atur cookie aplikasi Anda dengan atribut SameSite untuk membatasi pengiriman cookie hanya pada permintaan yang berasal dari domain yang sama. Ini akan membantu mencegah serangan CSRF dengan membatasi akses cookie dari domain lain.
5. Implementasikan Verifikasi Aksi: Pertimbangkan untuk menambahkan langkah verifikasi tambahan, seperti meminta pengguna untuk memasukkan kata sandi atau tindakan otorisasi tambahan sebelum mengizinkan aksi yang penting atau sensitif.
6. Lindungi API: Jika aplikasi web Anda memiliki API yang dapat diakses secara publik, pastikan bahwa API juga dilindungi dari serangan CSRF dengan menerapkan token CSRF dan validasi referer pada permintaan API.
7. Lakukan Pengujian Keamanan: Selalu lakukan pengujian keamanan secara rutin untuk mengidentifikasi potensi kerentanan CSRF pada aplikasi web Anda. Hal ini meliputi

pengujian penetrasi, pengujian fungsional, dan pengujian keamanan kode.

8. Pelatihan Pengguna: Edukasi pengguna tentang serangan CSRF dan cara menghindarinya. Berikan pemahaman kepada pengguna tentang pentingnya tidak membuka tautan yang mencurigakan atau menjalankan aksi yang tidak mereka kenali atau tidak diinginkan pada aplikasi web.

8.7.4 Serangan DDoS (*Distributed Denial of Service*)

Berikut ini adalah beberapa langkah pencegahan yang dapat Anda terapkan untuk melindungi sistem dan jaringan Anda dari serangan DDoS (*Distributed Denial of Service*):

1. Implementasikan Firewall yang Kuat: Gunakan firewall yang kuat untuk memfilter lalu lintas masuk dan keluar dari jaringan Anda. Firewall dapat memblokir lalu lintas yang mencurigakan atau yang berasal dari sumber yang tidak dikenal.
2. Gunakan Solusi Anti-DDoS: Pertimbangkan untuk menggunakan solusi anti-DDoS yang dirancang khusus untuk mendeteksi dan merespons serangan DDoS. Solusi ini dapat membantu mengidentifikasi pola lalu lintas yang mencurigakan dan menghalangi serangan sebelum mereka mencapai target.
3. Pemantauan Lalu lintas Jaringan: Lakukan pemantauan lalu lintas jaringan secara aktif untuk mendeteksi anomali atau peningkatan tiba-tiba dalam lalu lintas. Hal ini dapat membantu Anda mengidentifikasi serangan DDoS sejak dini dan mengambil tindakan yang tepat.
4. Konfigurasi Firewall dan Router: Pastikan firewall dan router Anda dikonfigurasi dengan baik untuk menghadapi serangan DDoS. Gunakan metode seperti pembatasan

bandwidth, pembatasan koneksi, atau pembatasan permintaan kecil yang berlebihan (*small packet attacks*).

5. Diversifikasi Infrastruktur: Mempertimbangkan diversifikasi infrastruktur dengan menggunakan beberapa penyedia layanan hosting atau menggunakan layanan CDN (*Content Delivery Network*). Dengan menggunakan infrastruktur yang terdistribusi, serangan DDoS dapat tersebar ke beberapa sumber daya, mengurangi dampak serangan pada satu titik.
6. Peringkat IP dan Blokir Serangan: Identifikasi IP yang terlibat dalam serangan DDoS dan blokir akses dari IP tersebut menggunakan firewall atau solusi keamanan jaringan lainnya. Juga, pertimbangkan untuk memanfaatkan layanan penyedia yang menawarkan perlindungan DDoS yang dapat memblokir lalu lintas berbahaya sebelum mencapai infrastruktur Anda.
7. Rencana Darurat dan Tanggap Krisis: Siapkan rencana darurat dan tanggap krisis yang terperinci untuk menghadapi serangan DDoS. Rencana ini harus mencakup langkah-langkah yang akan diambil untuk memulihkan layanan, menginformasikan pelanggan atau pengguna, dan melakukan investigasi pasca-serangan.
8. Peningkatan Kapasitas dan Redundansi: Pastikan infrastruktur Anda memiliki kapasitas yang cukup untuk menangani lonjakan lalu lintas yang tidak normal yang mungkin terjadi selama serangan DDoS. Selain itu, pertimbangkan untuk memiliki sistem redundan atau cadangan yang dapat diaktifkan jika satu sistem mengalami kegagalan.
9. Pendidikan dan Pelatihan Pengguna: Edukasi pengguna dan karyawan tentang serangan DDoS, pentingnya keamanan jaringan, dan tanda-tanda serangan DDoS.

Pelatihan ini dapat membantu mereka mengenali serangan dan melaporkannya dengan cepat.

10. Perbarui dan Lindungi Sistem: Pastikan semua sistem dan perangkat lunak Anda diperbarui secara

8.7.5 Serangan Brute Force

Berikut ini adalah beberapa langkah pencegahan yang dapat Anda terapkan untuk melindungi akun dan sistem Anda dari serangan *Brute Force*:

1. Gunakan Kata Sandi yang Kuat: Gunakan kata sandi yang kuat dan kompleks yang terdiri dari kombinasi huruf besar dan kecil, angka, dan karakter khusus. Hindari penggunaan kata sandi yang mudah ditebak atau umum seperti tanggal lahir atau nama depan.
2. Gunakan Autentikasi Dua Faktor (2FA): Aktifkan fitur autentikasi dua faktor (2FA) di akun Anda. Dengan 2FA, Anda akan memerlukan faktor kedua seperti kode yang dikirimkan melalui SMS, aplikasi autentikasi, atau perangkat keamanan fisik selain kata sandi untuk mengakses akun Anda.
3. Batasi Percobaan Masuk: Terapkan kebijakan pembatasan percobaan masuk dengan mengunci akun setelah beberapa percobaan yang gagal. Ini akan membatasi jumlah percobaan yang dapat dilakukan oleh penyerang dalam mencoba kata sandi yang benar.
4. Perbarui Perangkat Lunak: Selalu perbarui perangkat lunak sistem dan aplikasi Anda ke versi terbaru. Pembaruan perangkat lunak sering mengatasi kerentanan keamanan yang dapat dimanfaatkan oleh serangan Brute Force.
5. Monitoring Aktivitas Akun: Lakukan pemantauan aktivitas akun secara teratur untuk mendeteksi aktivitas yang mencurigakan atau upaya serangan. Perhatikan log

aktivitas dan periksa jika ada aktivitas login yang mencurigakan atau tidak dikenali.

6. Gunakan Solusi Perlindungan: Pertimbangkan untuk menggunakan solusi perlindungan keamanan yang khusus dirancang untuk mendeteksi dan mencegah serangan Brute Force. Solusi ini dapat mengenali pola lalu lintas mencurigakan dan memblokir serangan sebelum mencapai target.
7. Edukasi Pengguna: Edukasi pengguna tentang praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat, pengaktifan 2FA, dan pentingnya melindungi informasi pribadi. Pengguna yang sadar akan risiko serangan Brute Force akan lebih cenderung mengambil langkah-langkah keamanan yang tepat.
8. Tinjau Kebijakan Kata Sandi: Tinjau kebijakan kata sandi dalam organisasi Anda. Pastikan kebijakan tersebut mendorong pengguna untuk menggunakan kata sandi yang kuat dan mengubahnya secara berkala.
9. Batasi Akses yang Tidak Perlu: Batasi akses pengguna hanya pada level yang diperlukan. Jika seorang pengguna tidak membutuhkan akses tertentu, tidak ada alasan untuk memberikan hak akses tersebut yang dapat dieksploitasi oleh serangan Brute Force.
10. Monitoring Keamanan Jaringan: Lakukan monitoring keamanan jaringan secara aktif untuk mendeteksi aktivitas mencurigakan atau lalu lintas yang tidak normal yang dapat menjadi tanda serangan Brute Force.

8.7.6 Serangan *Man-in-the-Middle* (MitM)

Berikut adalah beberapa langkah pencegahan yang dapat Anda ambil:

1. Gunakan Koneksi yang Aman:
    a. Hindari menggunakan jaringan Wi-Fi publik atau tidak terpercaya. Jika Anda harus mengakses internet melalui Wi-Fi publik, gunakan Virtual Private Network (VPN) untuk membuat koneksi yang terenkripsi.
    b. Pastikan menggunakan situs web yang menggunakan protokol HTTPS dengan sertifikat SSL/TLS yang valid.
2. Perhatikan Tanda-tanda Keamanan:
    a. Periksa apakah alamat URL dimulai dengan "https://" dan adanya ikon gembok pada bilah alamat browser.
    b. Waspadai pesan peringatan yang muncul saat mengunjungi situs web yang mungkin tidak aman.
3. Lindungi Perangkat Anda:
    a. Selalu perbarui sistem operasi dan perangkat lunak dengan patch keamanan terbaru.
    b. Pasang dan perbarui perangkat lunak keamanan, seperti firewall dan antivirus.
4. Perhatikan Serangan Phishing:
    a. Jaga kehati-hatian saat menerima email atau pesan yang mencurigakan. Hindari mengklik tautan atau mengunduh lampiran dari sumber yang tidak dikenal atau mencurigakan.
    b. Periksa URL sebelum memasukkan informasi pribadi atau rahasia.
5. Gunakan Teknologi Keamanan Tambahan:
    a. Aktifkan verifikasi dua faktor (2FA) di akun-akun online Anda untuk mengamankan akses dan transaksi.
    b. Gunakan alat dan layanan keamanan, seperti *intrusion detection system* (IDS) atau *intrusion prevention system*

(IPS), yang dapat mendeteksi dan mencegah serangan MitM.

6. Edukasi Pengguna:
    1. Berikan pelatihan dan kesadaran keamanan kepada pengguna agar mereka dapat mengenali tanda-tanda serangan MitM dan mengambil langkah-langkah pencegahan yang tepat. (Pangestu & Liza, 2022)

8.7.7 Serangan Pharming

Untuk mengatasi serangan Pharming, berikut adalah beberapa langkah yang dapat diambil:

1. Gunakan DNS yang Aman: Gunakan layanan DNS yang aman dan terpercaya. Pastikan penyedia DNS Anda menggunakan metode pengamanan seperti DNSSEC (*Domain Name System Security Extensions*) yang memverifikasi integritas data DNS dan mencegah serangan Pharming.
2. Perbarui Perangkat Lunak: Selalu perbarui sistem operasi, perangkat lunak antivirus, dan perangkat jaringan Anda dengan patch keamanan terbaru. Ini akan membantu melindungi dari kerentanan yang diketahui yang dapat dimanfaatkan oleh serangan Pharming.
3. Monitor DNS dan Konfigurasi Jaringan: Periksa secara rutin pengaturan DNS pada server DNS Anda atau router jaringan Anda. Periksa juga konfigurasi jaringan dan pastikan tidak ada perubahan yang tidak sah atau tidak dikenal. Jika Anda mencurigai adanya perubahan, perbaiki pengaturan DNS atau hubungi penyedia layanan jaringan Anda.
4. Perhatikan Sertifikat SSL: Pastikan situs web yang Anda kunjungi memiliki sertifikat SSL yang valid. Periksa apakah ada tanda kunci keamanan di bilah alamat browser dan

pastikan URL situs web dimulai dengan "https://". Hal ini membantu mencegah pengalihan ke situs web palsu.

5. Gunakan Firewall dan Perangkat Lunak Keamanan: Aktifkan firewall pada perangkat jaringan Anda dan gunakan perangkat lunak keamanan yang terkini, seperti perangkat lunak antivirus, antispyware, dan antimalware. Ini akan membantu mendeteksi dan mencegah infeksi malware yang dapat digunakan dalam serangan Pharming.
6. Edukasi Pengguna: Tingkatkan kesadaran pengguna tentang serangan Pharming dan berbagi praktik terbaik dalam menjaga keamanan online. Beri tahu mereka tentang potensi serangan Pharming dan pentingnya memverifikasi URL dan sertifikat SSL sebelum memasukkan informasi sensitif.
7. Gunakan VPN (*Virtual Private Network*): Menggunakan VPN dapat membantu melindungi koneksi internet Anda dari serangan Pharming dengan mengenkripsi data yang dikirim antara perangkat Anda dan server tujuan. Ini membuat lebih sulit bagi penyerang untuk memanipulasi data DNS. (Sari *et al.*, 2022)

8.7.8 Serangan File Inclusion

Untuk mencegah serangan File Inclusion, berikut adalah beberapa langkah yang dapat diambil:

1. Validasi Input: Lakukan validasi input dengan cermat sebelum menggunakannya untuk memasukkan file. Periksa jenis data yang diharapkan, batasi karakter yang diperbolehkan, dan pastikan bahwa input yang diterima sesuai dengan aturan yang ditetapkan.
2. Escape atau Filter Karakter Khusus: Saat mengolah parameter input yang digunakan untuk menyertakan file, pastikan untuk menghindari interpretasi karakter khusus yang dapat dieksploitasi oleh penyerang. Gunakan teknik

seperti escaping atau filtering untuk menghindari potensi serangan.

3. Batasi Akses File Lokal: Terapkan pembatasan akses file lokal yang ketat pada server. Hindari memberikan akses yang tidak perlu pada file yang sensitif atau penting. Gunakan mekanisme seperti permission yang tepat untuk mengontrol akses file.
4. Gunakan Whitelist: Gunakan pendekatan whitelist untuk membatasi file yang dapat diakses atau disertakan dalam aplikasi web. Buat daftar putih file yang valid dan pastikan hanya file-file tersebut yang diizinkan untuk disertakan. Hindari menggunakan pendekatan blacklist yang rentan terhadap celah atau kelalaian.
5. Batasi Hak Akses: Pastikan bahwa aplikasi web berjalan dengan hak akses yang minimal. Berikan izin yang tepat pada file dan direktori yang diperlukan, tetapi hindari memberikan izin yang berlebihan yang dapat dimanfaatkan oleh penyerang.
6. Update dan Patch Sistem: Pastikan sistem operasi, server web, dan aplikasi yang digunakan selalu diperbarui dengan patch terbaru. Pembaruan ini sering kali mengatasi kerentanan keamanan yang ditemukan dalam sistem.
7. Periksa Konfigurasi Server: Periksa konfigurasi server web Anda untuk memastikan bahwa opsi yang berpotensi berbahaya seperti allow_url_include atau allow_url_fopen dinonaktifkan atau dikonfigurasi dengan baik.
8. Gunakan *Web Application Firewall* (WAF): Pertimbangkan untuk menggunakan *Web Application Firewall* (WAF) yang dapat mendeteksi dan mencegah serangan File Inclusion. WAF dapat memfilter dan menganalisis lalu lintas web untuk mendeteksi pola serangan yang mencurigakan.
9. Lakukan Audit Keamanan Reguler: Lakukan audit keamanan rutin untuk mengidentifikasi dan mengatasi

kerentanan yang ada. Periksa aplikasi web secara berkala untuk memastikan tidak ada celah keamanan yang dapat dimanfaatkan.

10. Tingkatkan Kesadaran Pengguna: Tingkatkan kesadaran pengguna tentang ancaman keamanan, seperti serangan File Inclusion. Berikan pelatihan keamanan kepada pengembang dan pengguna agar mereka memahami potensi serangan dan tindakan pencegahan yang dapat diambil.

8.7.9 Serangan *Server Side Request Forgery* (SSRF)

Untuk mengatasi serangan SSRF, berikut adalah beberapa langkah yang dapat diambil:

1. Validasi Input: Lakukan validasi yang ketat terhadap input yang diterima oleh aplikasi web. Pastikan bahwa input yang diberikan adalah URL yang valid dan tidak mengandung karakter atau skema yang tidak diharapkan.
2. Whitelist atau Blacklist: Buat daftar putih (*whitelist*) atau daftar hitam (*blacklist*) untuk mengontrol sumber daya yang dapat diakses oleh server aplikasi. Daftar putih mencantumkan URL yang diperbolehkan untuk diakses, sementara daftar hitam mencantumkan URL yang dilarang diakses. Ini membantu memastikan bahwa server hanya dapat membuat permintaan ke sumber daya yang diizinkan.
3. Pembatasan Jaringan: Batasi akses server aplikasi ke sumber daya internal atau jaringan lokal. Konfigurasikan firewall atau pengaturan jaringan yang tepat untuk membatasi akses yang diperbolehkan dari server aplikasi. Hal ini membantu mencegah server aplikasi mengakses sumber daya yang tidak seharusnya dapat diakses.
4. Sanitisasi Input: Pastikan untuk membersihkan dan menyaring input pengguna sebelum menggunakannya

dalam pembuatan permintaan HTTP. Hindari penggunaan input pengguna dalam URL langsung atau dalam parameter permintaan HTTP tanpa sanitasi yang tepat. Gunakan fungsi sanitasi atau pembersihan data untuk memastikan bahwa input yang diterima tidak mengandung karakter atau skema yang tidak diinginkan.

5. Batasan Perizinan: Terapkan batasan perizinan yang ketat untuk mengontrol jenis permintaan yang dapat dilakukan oleh server aplikasi. Batasi jenis permintaan yang dapat dilakukan, seperti hanya memperbolehkan permintaan HTTP GET atau membatasi penggunaan protokol khusus seperti file://.
6. Monitoring dan Logging: Pantau aktivitas server aplikasi secara teratur dan periksa log untuk mendeteksi indikasi serangan SSRF. Perhatikan permintaan yang mencurigakan, seperti permintaan ke sumber daya internal yang tidak diharapkan atau permintaan dengan URL yang mencurigakan. Log aktivitas server dapat memberikan wawasan yang berharga tentang kemungkinan serangan SSRF.
7. Pembaruan dan *Patches*: Pastikan bahwa sistem operasi, perangkat lunak, dan kerangka kerja yang digunakan dalam aplikasi web selalu diperbarui dengan versi terbaru. Pembaruan dan patch seringkali mengatasi kerentanan keamanan yang dapat dimanfaatkan dalam serangan SSRF.
8. Kesadaran Pengguna: Berikan pelatihan dan kesadaran keamanan kepada pengguna tentang potensi serangan SSRF. Beritahu mereka tentang risiko yang terlibat dalam mengklik tautan atau mengirim permintaan ke sumber daya yang tidak dikenal atau tidak terpercaya.

8.7.10 Serangan Clickjacking

Berikut adalah beberapa langkah-langkah pencegahan untuk melindungi situs web dari serangan Clickjacking:

1. Implementasikan header HTTP "X-Frame-Options": Gunakan header HTTP "X-Frame-Options" dengan nilai "DENY" atau "SAMEORIGIN" untuk mengontrol apakah halaman web dapat dimuat dalam bingkai (*frame*) di luar domain asal. Nilai "DENY" akan mencegah penggunaan bingkai secara keseluruhan, sementara nilai "SAMEORIGIN" membatasi bingkai hanya pada domain yang sama.
2. Gunakan Content Security Policy (CSP): Implementasikan kebijakan keamanan konten (CSP) yang sesuai untuk membatasi sumber daya yang dapat dimuat dalam halaman web. Dalam kebijakan CSP, Anda dapat mengatur kebijakan "frame-ancestors" yang membatasi domain yang diperbolehkan untuk memuat halaman web dalam bingkai. Dengan demikian, Anda dapat mencegah penanaman halaman web dalam bingkai yang tidak diizinkan.
3. Implementasikan *JavaScript Framebusting*: Framebusting adalah teknik yang menggunakan JavaScript untuk mendeteksi apakah halaman web sedang dimuat dalam bingkai dan menghentikan proses loading jika demikian. Anda dapat mengimplementasikan kode JavaScript seperti berikut ini di setiap halaman web untuk melindunginya dari serangan Clickjacking. (Jaelani & Khoirunnisa, 2023)

DAFTAR PUSTAKA

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. 2021. Web application penetration testing using sql injection attack. *International Journal on Informatics Visualization*, *5*(3), 320–326. https://doi.org/10.30630/joiv.5.3.470

Haryanto, D. 2017. *Sistem Informasi Pariwisata Di Kabupaten Kebumen Berbasis Web*. *2*(1), 10–17. https://eprints.akakom.ac.id/4915/%0Ahttps://eprints.akakom.ac.id/4915/1/01_145610189_HALAMAN_DEPAN.pdf

Hasibuan, M., & Elhanafi, A. M. 2022. Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Herdiana, Y., & Saepudin, D. S. 2023. *Perancangan Sistem Informasi Penjualan Menggunakan Cms Wordpress Berbasis Web (Di Sandallaku Majalaya)*. *05*, 55–62.

Hudaya, A., & Primananda, R. 2023. *Analisis Perbandingan Dampak Serangan Distributed Denial of Service pada Protokol Routing OSPF dan IS-IS*. *7*(4), 1656–1661.

Iqbal Kurniansyah, M., & Sinurat, S. 2020. Sistem Pendukung Keputusan Pemilihan Server Hosting dan Domain Terbaik untuk WEB Server Menerapkan Metode VIKOR. *JSON (Jurnal Sistem Komputer Dan Informatika)*, *2*(1), 14–24. https://doi.org/10.30865/json.v2i1.2450

Jaelani, W. L., & Khoirunnisa, F. 2023. *Penetration Testing Website Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan Website Pada Instansi (Redacted)*. *05*(01), 1–8.

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. 2022. Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi kasus:RS H.LMANAMBAI ABDULKADIR). *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mushlih, M., Fitri, R., & Wardiah, I. 2019. Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Seminar Nasional Riset …*, *5662*(November), 41–47. http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409

Pangestu, T., & Liza, R. 2022. Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing. *JiTEKH*, *10*(2), 60–67. https://doi.org/10.35447/jitekh.v10i2.571

Putra, Y., Yuhandri, Y., & Sumijan, S. 2021. Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

Quispe, J. 2023. No Title**การบริหารจัดการการบริการที่มีคุณภาพในโรงพยาบาลสังกัดกระทรวงสาธารณสุข**. ***วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย***, *4*(1), 88–100.

Ramaddan Julianti, M., Akas Suwandara, J., Ali Akbar Jufri, M., Nabili Akbar, R., Abdul Hakim, R., & Diva Wardana, R. P. 2022. *Membuat Blog Dengan Wordpress (Hosting Dan Domain Gratis) Pada Siswa Smkn 2 Kab. Tangerang Article History*. *1*(2), 1.

Salamah, U., & Khasanah, F. N. 2017. Pengujian Sistem Informasi Penjualan Undangan Pernikahan Online Berbasis Web Menggunakan Black Box Testing. *Information Management for Educators and Professionals*, *2*(1), 35–46.

Sari, E. P., Febrianti, D. A., & ... 2022. Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory. *Deviance Jurnal …*, *6*, 153–168. https://journal.budiluhur.ac.id/index.php/deviance/article/view/1882%0Ahttps://journal.budiluhur.ac.id/index.php/deviance/article/download/1882/1272

Sie, J. B. L., Izmy Alwiah Musdar, & Syamsul Bahri. 2022. Pengujian White Box Testing Terhadap Website Room Menggunakan Teknik Basis Path. *KHARISMA Tech*, *17*(2), 45–57. https://doi.org/10.55645/kharismatech.v17i2.235

Utami Aulia Alma. 2018. *Analisis model bisnis pada bisnis*. *5*(2), 2538–2546.

Wang, E., Wang, B., Xie, W., Wang, Z., Luo, Z., & Yue, T. 2020. EWVHunter: Grey-box fuzzing with knowledge guide on embedded web front-ends. *Applied Sciences (Switzerland)*, *10*(11). https://doi.org/10.3390/app10114015

Zirwan, A. 2022. Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi Dan Teknologi*, *4*(1), 70–75. https://doi.org/10.37034/jidt.v4i1.190

BAB 9
IP (INTERNET PROTOCOL) SECURITY

Oleh Arief Yanto Rukmana

9.1 Pendahuluan

Di dunia yang saling terhubung saat ini (Wakil et al., 2022), di mana informasi dipertukarkan secara global dengan kecepatan yang belum pernah terjadi sebelumnya (Rukmana, 2023), memastikan keamanan dan integritas transmisi data menjadi hal yang terpenting (Lalit *et al.,* 2022). Salah satu blok bangunan fundamental dari jaringan modern adalah Internet Protocol (IP), yang berfungsi sebagai dasar untuk merutekan dan mengirimkan paket data melalui jaringan (Yaroub *et al*., n.d.). Namun, sifat jaringan IP yang terbuka dan terdistribusi menimbulkan tantangan keamanan yang signifikan (Tamsir Ariyadi, 2022), menjadikan keamanan IP sebagai aspek penting dari keamanan informasi (Puspita et al., 2022).

Keamanan IP mencakup berbagai teknik, protokol, dan mekanisme yang dirancang untuk melindungi komunikasi berbasis IP dari akses tidak sah, manipulasi data, dan serangan jaringan (Mughal, 2022). Ini bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data saat melintasi sistem yang saling terhubung, melindungi privasi individu dan organisasi (Harto et al., 2022), dan menjaga kepercayaan ekosistem digital (Noviantoro, 2022).

Keamanan IP melibatkan penerapan berbagai protokol dan teknologi untuk membangun saluran komunikasi yang aman, mengautentikasi entitas, mengenkripsi data, mendeteksi dan

mencegah intrusi jaringan, dan mengurangi potensi kerentanan dan ancaman (Kaeo, 2004). Dengan menerapkan langkah-langkah keamanan IP yang kuat, organisasi dapat melindungi jaringan mereka dari aktivitas jahat dan menjaga integritas dan kerahasiaan informasi sensitive (Munawar & Putri, 2020).

Keamanan IP mencakup beragam elemen, termasuk enkripsi, kontrol akses, otentikasi, dan pemantauan jaringan. Ini memanfaatkan protokol standar industri seperti IPsec, *Secure Sockets Layer/Transport Layer Security* (SSL/TLS), dan *Secure Shell* (SSH) untuk menyediakan mekanisme keamanan yang kuat untuk komunikasi berbasis IP.

Ancaman terhadap jaringan IP sangat banyak dan terus berkembang (Marin, 2005). Peretas, penjahat dunia maya, dan aktor jahat lainnya terus-menerus mengeksploitasi kerentanan dalam infrastruktur jaringan untuk mendapatkan akses tidak sah, mencegat data sensitif, mengganggu layanan, dan meluncurkan serangan dahsyat seperti *Distributed Denial of Service* (DDoS). Selain itu, proliferasi jaringan nirkabel dan *Internet of Things* (IoT) telah menghadirkan tantangan tambahan, karena memperluas permukaan serangan dan meningkatkan kompleksitas pengamanan komunikasi berbasis IP (Yu *et al.,* 2022).

Uraian dalam tulisan ini bertujuan untuk memberi pembaca pemahaman mendalam tentang prinsip dasar, protokol, dan teknik yang diperlukan untuk melindungi jaringan IP secara efektif. Ini akan mengeksplorasi dasar-dasar IP, ancaman dan serangan keamanan umum yang menargetkan komunikasi berbasis IP, protokol dan mekanisme keamanan yang digunakan untuk mengamankan lalu lintas IP, dan praktik terbaik untuk menerapkan langkah-langkah keamanan IP yang kuat.

Bagian bab ini akan menyelidiki seluk-beluk mengamankan jaringan IP, yang mencakup topik-topik seperti kontrol akses, firewall, deteksi intrusi dan sistem pencegahan, jaringan pribadi virtual, terjemahan alamat jaringan, segmentasi jaringan, dan zona

demiliterisasi. Selain itu, ini akan mengatasi tantangan spesifik terkait jaringan nirkabel dan *Internet of Things* (IoT), memeriksa pertimbangan keamanan unik dan penanggulangan yang diperlukan untuk lingkungan ini.

Di akhir uraian ini, pembaca akan memiliki pemahaman yang komprehensif tentang konsep dan teknik keamanan IP, yang memungkinkan mereka menerapkan langkah-langkah keamanan yang kuat dan melindungi jaringan mereka dari ancaman yang muncul. Baik Anda seorang administrator jaringan, profesional keamanan, atau manajer TI, buku ini akan membekali Anda dengan pengetahuan dan keterampilan yang diperlukan untuk melindungi komunikasi IP dan memastikan integritas dan kerahasiaan data di dunia yang saling terhubung saat ini.

9.2 Dasar-Dasar IP

Dasar-dasar IP (*Internet Protocol*) membentuk tulang punggung jaringan modern, memungkinkan perutean dan pengiriman paket data melalui jaringan yang saling terhubung (Marin, 2005). Pengalamatan IP berfungsi sebagai pengidentifikasi unik untuk perangkat di jaringan, memungkinkan komunikasi tanpa batas. IPv4, versi yang paling banyak digunakan, menggunakan struktur biner 32-bit, dengan alamat yang direpresentasikan dalam notasi desimal bertitik desimal. Kelas alamat (A, B, C, D, E) dan subnetting memberikan fleksibilitas dalam desain jaringan dan penggunaan ruang alamat yang efisien. Alamat IP pribadi, dicadangkan untuk jaringan internal, dipetakan ke alamat IP publik melalui *Network Address Translation* (NAT) untuk mengakses internet. Sebaliknya, alamat IPv6 menawarkan struktur biner 128-bit yang diperluas, memungkinkan sejumlah besar alamat unik untuk memenuhi permintaan perangkat yang terhubung yang terus meningkat.

Manajemen alamat IP melibatkan berbagai metode untuk penetapan alamat, termasuk alokasi statis dan penetapan dinamis

melalui protokol seperti DHCP. Manajemen alamat IP yang efektif mencakup perencanaan, dokumentasi, dan pelacakan alamat IP untuk memelihara infrastruktur jaringan yang terorganisir. Selain itu, resolusi alamat IP dicapai melalui protokol seperti ARP (*Address Resolution Protocol*) di IPv4 dan NDP (*Neighbor Discovery Protocol*) di IPv6, menerjemahkan alamat IP ke alamat MAC untuk komunikasi yang efisien dalam jaringan lokal. Segmentasi jaringan, dicapai melalui subnetting dan VLAN, meningkatkan keamanan, kinerja, dan alokasi sumber daya dengan memisahkan segmen jaringan secara logis dan fisik (Pamarthi & Narmadha, 2022).

Memahami dasar-dasar pengalamatan IP sangat penting bagi administrator jaringan, arsitek, dan insinyur. Ini memungkinkan desain jaringan yang tepat, alokasi alamat yang efisien, dan kemampuan untuk memecahkan masalah konektivitas. Dengan transisi ke IPv6 dan pertumbuhan berkelanjutan dari perangkat yang terhubung, pemahaman yang kuat tentang dasar-dasar IP sangat penting untuk membangun jaringan yang kuat dan dapat diskalakan. Dengan menerapkan praktik manajemen alamat IP yang efektif, organisasi dapat memastikan pemanfaatan sumber daya yang efisien dan memelihara infrastruktur jaringan yang aman dan andal (Hassan, 2022).

9.2.1 Struktur Paket IP

Struktur paket IP merupakan salah satu aspek fundamental dalam jaringan komputer, yang memungkinkan pengiriman data secara efisien dan akurat melalui jaringan yang saling terhubung. Setiap paket data yang dikirim melalui jaringan menggunakan protokol IP, dan setiap paket tersebut memiliki struktur yang terdiri dari beberapa bagian yang penting (Hananto, 2023).

Pertama-tama, paket IP terdiri dari header dan payload. Header berisi informasi penting yang diperlukan untuk mengarahkan paket ke tujuan yang tepat, sedangkan payload berisi data aktual yang akan dikirimkan. Header paket IP memiliki panjang tetap, yaitu 20 byte untuk IPv4 dan 40 byte untuk IPv6.

Di dalam header, terdapat beberapa field yang memiliki fungsi spesifik. Salah satu field yang penting adalah field versi, yang menunjukkan versi protokol IP yang digunakan, apakah itu IPv4 atau IPv6. Selain itu, terdapat field panjang header, yang menunjukkan panjang total dari header tersebut. Field ini diperlukan untuk mengatur proses fragmentasi dan reasembli paket, jika diperlukan (Rahardjo, 2005).

Field lainnya adalah field alamat IP pengirim dan penerima, yang menunjukkan alamat IP sumber dan tujuan paket. Informasi ini sangat penting dalam proses routing paket melalui jaringan. Terdapat juga field *Time to Live* (TTL), yang menentukan batasan jumlah hop atau node yang dapat dilalui oleh paket sebelum dihapus dari jaringan. Field ini mencegah terjadinya loop tak terbatas di dalam jaringan (Dara et al., 2023).

Selanjutnya, terdapat field jenis layanan (TOS) yang digunakan untuk menandai prioritas dan kualitas layanan dari paket. Field ini dapat digunakan untuk mengatur pengiriman paket yang sensitif terhadap delay atau paket yang membutuhkan prioritas tertentu.

Pada bagian akhir header, terdapat field checksum, yang digunakan untuk memastikan integritas data paket IP. Checksum ini dihitung berdasarkan semua field header, sehingga dapat mendeteksi adanya kesalahan dalam pengiriman paket.

Diikuti oleh header, terdapat payload yang berisi data aktual yang akan dikirimkan melalui jaringan. Payload ini bisa berupa data dari protokol transport seperti TCP atau UDP, atau data dari protokol aplikasi seperti HTTP atau FTP.

Memahami struktur paket IP secara mendalam memungkinkan para profesional jaringan untuk melakukan analisis, pemecahan masalah, dan optimisasi jaringan dengan lebih efektif (Jamaluddin & Siringoringo, 2023). Dengan pengetahuan tentang struktur paket IP, mereka dapat mengidentifikasi masalah jaringan, melakukan monitoring dan analisis lalu lintas jaringan, serta mengoptimalkan

proses routing dan pengiriman data. Struktur paket IP menjadi dasar yang penting dalam memahami cara kerja jaringan komputer dan memastikan pengiriman data yang aman dan efisien.

9.3 Ancaman dan Serangan Keamanan IP

Ancaman dan serangan keamanan IP menimbulkan risiko yang signifikan terhadap kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui jaringan IP. Memahami ancaman ini sangat penting untuk menerapkan langkah-langkah keamanan yang efektif (Choubey *et al*., 2022).

Salah satu ancaman keamanan IP yang paling umum adalah akses tidak sah, di mana penyerang mendapatkan akses tidak sah ke jaringan atau sistem. Ini dapat menyebabkan pelanggaran data, manipulasi data yang tidak sah, dan pelanggaran privasi. Penyerang sering mengeksploitasi kerentanan pada perangkat jaringan, sistem operasi, atau aplikasi untuk mendapatkan akses. Mereka mungkin menggunakan teknik seperti peretasan kata sandi, serangan brute force, atau mengeksploitasi kerentanan perangkat lunak (Taghizad-Tavana *et al.,* 2022).

Ancaman utama lainnya adalah penyadapan jaringan, di mana penyerang mencegat dan menangkap lalu lintas jaringan untuk mendapatkan akses ke informasi sensitif. Ini dapat dilakukan melalui teknik seperti packet sniffing, di mana penyerang menangkap dan menganalisis paket jaringan untuk mengekstrak data seperti kredensial login, informasi keuangan, atau data bisnis rahasia. Serangan penyadapan dapat sangat merugikan di lingkungan jaringan yang tidak terenkripsi, di mana data ditransmisikan dalam teks biasa (DeNardis, 2022).

Jaringan IP juga rentan terhadap berbagai jenis serangan jaringan. Serangan *Distributed Denial of Service* (DDoS) membanjiri jaringan atau sistem target dengan jumlah lalu lintas yang sangat banyak, membuatnya tidak tersedia untuk pengguna yang sah. Serangan ini dapat mengganggu operasi bisnis, menyebabkan

kerugian finansial, dan merusak reputasi organisasi. Serangan jaringan lainnya termasuk spoofing IP, di mana penyerang memanipulasi alamat IP sumber untuk menipu penerima dan melewati langkah-langkah keamanan, dan serangan man-in-the-middle, di mana penyerang mencegat dan mengubah komunikasi antara dua pihak (VARGA & KUJUNDZIC, 2022).

Ancaman keamanan IP juga meluas ke kerentanan dalam protokol dan layanan. Misalnya, serangan fragmentasi IP mengeksploitasi kerentanan dalam proses fragmentasi dan perakitan ulang IP, menyebabkan kemacetan jaringan, kehabisan sumber daya, atau penghindaran kontrol keamanan. Serangan peracunan *Address Resolution Protocol* (ARP) memanipulasi tabel ARP untuk mengalihkan lalu lintas jaringan ke sistem penyerang, memungkinkan akses tidak sah dan intersepsi data.

Jaringan IP menghadapi tantangan keamanan dari teknologi baru seperti jaringan nirkabel dan *Internet of Things* (IoT). Mekanisme autentikasi yang lemah, konfigurasi yang tidak aman, dan kurangnya pembaruan firmware membuat jaringan nirkabel rentan terhadap akses tidak sah, penyadapan data, dan serangan. Perangkat IoT, sering digunakan dengan langkah-langkah keamanan yang tidak memadai, dapat disusupi untuk meluncurkan serangan pada jaringan IP atau menjadi target penyerang yang ingin mendapatkan akses tidak sah ke sistem penting (Forouzan & Mukhopadhyay, 2015).

Ancaman dan serangan keamanan IP menimbulkan risiko yang signifikan terhadap kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui jaringan IP. Sangat penting bagi organisasi untuk menyadari ancaman ini dan menerapkan langkah-langkah keamanan yang kuat untuk melindungi jaringan mereka. Ini termasuk menggunakan kontrol akses yang kuat, mekanisme enkripsi, deteksi intrusi dan sistem pencegahan, dan secara teratur memperbarui dan menambal perangkat dan perangkat lunak jaringan. Pendekatan proaktif dan komprehensif

terhadap keamanan IP sangat penting untuk memitigasi lanskap ancaman yang terus berkembang dan memastikan pengoperasian jaringan IP yang aman (Akter *et al.,* 2022).

9.4 Protokol Keamanan IP

Protokol keamanan IP memainkan peran penting dalam menjaga kerahasiaan, integritas, dan keaslian data yang dikirimkan melalui jaringan IP. Protokol ini menyediakan mekanisme untuk komunikasi yang aman, autentikasi, dan enkripsi untuk melindungi informasi sensitif dari akses dan gangguan yang tidak sah (Sen, 2013).

Salah satu protokol keamanan IP utama adalah IPsec (IP Security). IPsec adalah kerangka kerja protokol dan algoritme yang menyediakan komunikasi aman pada lapisan IP. Ia menawarkan dua layanan utama: *Authentication Header* (AH) dan *Encapsulating Security Payload* (ESP). AH memastikan integritas dan otentikasi data dengan menambahkan tanda tangan digital ke paket IP, memverifikasi identitas pengirim dan mendeteksi setiap modifikasi. ESP, di sisi lain, menyediakan enkripsi dan otentikasi, melindungi muatan paket IP dari penyadapan dan akses tidak sah.
Protokol keamanan IP penting lainnya adalah *Secure Socket Layer*/*Transport Layer Security* (SSL/TLS). Meskipun terutama terkait dengan mengamankan komunikasi web (HTTPS), SSL/TLS dapat digunakan untuk mengamankan berbagai protokol berbasis IP. Protokol SSL/TLS membangun koneksi terenkripsi antara klien dan server, memastikan kerahasiaan dan integritas data yang dikirimkan melalui jaringan. Mereka menggunakan kombinasi algoritma enkripsi simetris dan asimetris, seperti RSA dan AES, untuk membangun saluran komunikasi yang aman dan mencegah penyadapan dan perusakan (Foruzan, 2007).

Internet Key Exchange (IKE) adalah protokol keamanan IP yang memfasilitasi pembentukan asosiasi keamanan IPsec. IKE menyediakan proses manajemen kunci yang aman dan otomatis,

memungkinkan komunikasi yang aman antara perangkat yang mendukung IPsec. Ini menegosiasikan algoritme kriptografi, menghasilkan kunci rahasia bersama, dan membuat saluran aman untuk bertukar paket IP terenkripsi. IKE menggunakan pertukaran kunci Diffie-Hellman dan sertifikat digital untuk mengautentikasi dan membangun saluran komunikasi yang aman (VARGA & KUJUNDZIC, 2022).

Transport Layer Security (TLS) adalah protokol yang digunakan untuk mengamankan komunikasi antara aplikasi yang berjalan di host yang berbeda. Ini beroperasi pada lapisan transport (misalnya, TCP) dan menyediakan pemeriksaan enkripsi, otentikasi, dan integritas untuk data dalam perjalanan. Protokol TLS memastikan komunikasi yang aman antara aplikasi seperti email, transfer file, dan jaringan pribadi virtual (VPN). Ini menggunakan kombinasi algoritma enkripsi simetris dan asimetris untuk mengamankan transportasi data, dan sertifikat digital untuk otentikasi dan pertukaran kunci (Indrawan, n.d.).

Selain itu, protokol *Virtual Private Network* (VPN), seperti *Point-to-Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), dan *Open*VPN, memanfaatkan IPsec dan mekanisme enkripsi lainnya untuk membangun koneksi yang aman melalui jaringan publik. Protokol VPN memungkinkan akses jarak jauh yang aman ke jaringan pribadi, membuat terowongan terenkripsi untuk melindungi data yang dikirimkan antara pengguna jarak jauh dan jaringan. Mereka memberikan kerahasiaan, integritas, dan otentikasi data, memastikan komunikasi dan privasi yang aman (Kizza, 2005).

Protokol keamanan IP memainkan peran penting dalam melindungi kerahasiaan, integritas, dan keaslian data yang dikirimkan melalui jaringan IP. Protokol seperti IPsec, SSL/TLS, IKE, protokol VPN, dan lainnya menyediakan mekanisme untuk komunikasi yang aman, enkripsi, autentikasi, dan manajemen kunci. Dengan menerapkan protokol ini, organisasi dapat membuat

saluran komunikasi yang aman, melindungi informasi sensitif dari akses tidak sah dan perusakan, serta memastikan privasi dan keamanan data yang dikirimkan melalui jaringan IP. Protokol-protokol ini membentuk dasar komunikasi yang aman di era digital, mengatasi tantangan keamanan yang berkembang yang dihadapi oleh jaringan modern (Aydos *et al.,* 1999).

9.5 Mekanisme Keamanan IP

Mekanisme keamanan IP mencakup berbagai teknik dan protokol yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data yang dikirimkan melalui jaringan IP. Mekanisme ini sangat penting untuk memastikan komunikasi yang aman dan mengurangi risiko yang ditimbulkan oleh akses tidak sah, intersepsi data, dan gangguan (Potlapally *et al.,* 2003).

Salah satu mekanisme keamanan IP mendasar adalah enkripsi, yang mengubah data teks biasa menjadi teks sandi menggunakan algoritme kriptografi. Enkripsi memastikan bahwa data tetap rahasia dan aman selama transmisi melalui jaringan IP, sehingga menyulitkan penyerang untuk menguraikan informasi tanpa kunci dekripsi yang sesuai. Algoritme enkripsi simetris, seperti *Advanced Encryption Standard* (AES), menggunakan kunci yang sama untuk enkripsi dan dekripsi, sementara algoritma enkripsi asimetris, seperti RSA, menggunakan sepasang kunci, satu untuk enkripsi dan satu lagi untuk dekripsi. Mekanisme enkripsi dapat diintegrasikan ke dalam protokol keamanan IP seperti IPsec atau SSL/TLS untuk menyediakan enkripsi end-to-end paket IP dan saluran komunikasi yang aman (Choubey *et al.,* 2022).

Otentikasi adalah mekanisme keamanan IP penting lainnya yang memverifikasi identitas pihak yang berkomunikasi dan memastikan integritas data yang dikirimkan. Berbagai mekanisme autentikasi, seperti sertifikat digital, token, atau sistem biometrik, dapat digunakan untuk mengautentikasi pengguna, perangkat, atau komponen jaringan. Mekanisme ini membantu mencegah akses

tidak sah dan perusakan data dengan memverifikasi keabsahan peserta dalam komunikasi IP.

Mekanisme kontrol akses memainkan peran penting dalam keamanan IP dengan memberlakukan pembatasan pada sumber daya jaringan dan menentukan siapa yang dapat mengakses data atau sistem tertentu. Daftar kontrol akses (ACL) dan aturan firewall biasanya digunakan untuk menentukan dan menegakkan kebijakan akses, yang memungkinkan organisasi mengontrol lalu lintas jaringan dan membatasi akses ke sumber daya sensitif. Sistem kontrol akses berbasis peran (RBAC) dan manajemen akses dan identitas (IAM) menyediakan kontrol terperinci atas izin dan hak istimewa pengguna, yang semakin meningkatkan keamanan.
Sistem deteksi dan pencegahan intrusi (IDPS) adalah mekanisme keamanan IP penting yang memantau lalu lintas jaringan untuk aktivitas mencurigakan dan potensi serangan. Sistem ini menggunakan berbagai teknik, seperti deteksi berbasis tanda tangan, deteksi anomali, dan analisis perilaku, untuk mengidentifikasi dan menanggapi insiden keamanan. IDPS dapat secara otomatis memblokir atau mengurangi ancaman, melindungi jaringan dari akses tidak sah, infeksi malware, dan aktivitas jahat lainnya (Kaeo, 2004; Marin, 2005).

Segmentasi jaringan adalah mekanisme keamanan IP yang membagi jaringan menjadi subnetwork yang lebih kecil, membatasi dampak pelanggaran keamanan potensial. Dengan memisahkan sistem dan data sensitif dari bagian jaringan lainnya, segmentasi jaringan mencegah pergerakan lateral dan meminimalkan jangkauan serangan. VLAN, subnet, dan jaringan pribadi virtual (VPN) biasanya digunakan untuk mencapai segmentasi jaringan dan meningkatkan keamanan.

Metode Kerja keamanan IP mencakup langkah-langkah untuk manajemen kunci yang aman, yang memastikan kerahasiaan dan integritas kunci enkripsi yang digunakan dalam komunikasi yang aman. Protokol distribusi kunci, seperti *Internet Key Exchange*

(IKE), memfasilitasi pertukaran aman kunci enkripsi antara pihak yang berkomunikasi. Sistem dan praktik manajemen kunci, termasuk pembuatan, rotasi, dan pencabutan kunci, membantu menjaga keamanan operasi kriptografi dan mencegah akses tidak sah ke data sensitive (DeNardis, 2022).

Mekanisme keamanan IP mencakup enkripsi, otentikasi, kontrol akses, deteksi dan pencegahan intrusi, segmentasi jaringan, dan manajemen kunci yang aman. Mekanisme ini secara kolektif menyediakan kerangka komprehensif untuk melindungi jaringan IP dan memastikan transmisi data yang aman. Dengan menerapkan dan mengintegrasikan mekanisme ini ke dalam infrastruktur jaringan, organisasi dapat membangun postur keamanan yang kuat, melindungi informasi sensitif, dan mengurangi risiko yang terkait dengan akses tidak sah, penyadapan data, dan perusakan. Mekanisme keamanan IP memainkan peran penting dalam membangun jaringan yang tangguh dan aman dalam menghadapi ancaman keamanan siber yang terus berkembang (Foruzan, 2007; Kizza, 2005).

9.6 Praktik Terbaik Keamanan IP

Menerapkan praktik terbaik keamanan IP sangat penting bagi organisasi untuk melindungi jaringan dan data sensitif mereka dari potensi ancaman dan serangan (Mughal, 2022). Praktik-praktik ini mencakup serangkaian tindakan dan pedoman yang meningkatkan postur keamanan jaringan IP dan mengurangi kerentanan (Hassan, 2022; Taghizad-Tavana *et al.,* 2022).

Pertama dan terpenting, pembaruan dan tambalan rutin harus diterapkan ke perangkat jaringan, sistem operasi, dan aplikasi. Ini membantu mengatasi kerentanan keamanan yang diketahui dan memastikan bahwa sistem dilengkapi dengan peningkatan keamanan terbaru. Manajemen patch tepat waktu sangat penting untuk mencegah eksploitasi kerentanan yang diketahui oleh penyerang (Mughal, 2022; Yaroub *et al.,* n.d.).

Kontrol akses yang kuat harus diterapkan untuk membatasi akses tidak sah ke sumber daya jaringan. Ini termasuk menegakkan penggunaan kata sandi yang rumit dan unik atau menerapkan mekanisme autentikasi multifaktor untuk akun pengguna. Hak akses harus ditetapkan berdasarkan kebutuhan untuk mengetahui, memastikan bahwa pengguna hanya memiliki akses ke sumber daya yang diperlukan untuk peran mereka.

Segmentasi jaringan adalah praktik yang efektif untuk membatasi dampak pelanggaran keamanan potensial. Dengan membagi jaringan menjadi segmen yang lebih kecil atau VLAN, organisasi dapat mengisolasi sistem dan data sensitif dari jaringan lainnya. Ini mengurangi permukaan serangan dan mencegah gerakan lateral dalam jaringan (Sadhu *et al.,* 2022).

Enkripsi harus digunakan untuk data sensitif saat transit, terutama melalui jaringan publik atau tidak tepercaya (Herman *et al.,* 2023; Yanto Rukmana *et al.,* 2021). Protokol IPsec, SSL/TLS, atau VPN dapat digunakan untuk membangun saluran komunikasi yang aman dan mengenkripsi paket data. Ini melindungi kerahasiaan dan integritas data yang dikirimkan melalui jaringan IP.

Pemantauan dan analisis rutin lalu lintas jaringan sangat penting untuk mengidentifikasi dan merespons potensi insiden keamanan. Sistem deteksi dan pencegahan intrusi (IDPS) harus dikerahkan untuk memantau aktivitas jaringan, mendeteksi perilaku yang mencurigakan atau tanda-tanda serangan, dan memicu tindakan respons yang sesuai. Selain itu, mekanisme pencatatan dan audit harus diaktifkan untuk menangkap dan menganalisis peristiwa jaringan untuk tujuan forensic (Holt *et al.,* 2022).

Organisasi harus memiliki cadangan yang kuat dan rencana pemulihan bencana untuk memastikan kelangsungan bisnis jika terjadi insiden keamanan atau kegagalan sistem. Mencadangkan data penting secara teratur dan menyimpan cadangan di luar lokasi

memberikan perlindungan terhadap kehilangan data dan memfasilitasi pemulihan jika terjadi pelanggaran atau kompromi system (Atlam *et al.,* 2020).

Program kesadaran dan pelatihan karyawan memainkan peran penting dalam keamanan IP. Karyawan harus dididik tentang praktik terbaik keamanan, termasuk kebersihan kata sandi, ancaman rekayasa sosial, dan kebiasaan menjelajah yang aman. Pelatihan kesadaran keamanan rutin membantu menumbuhkan budaya sadar keamanan dan memberdayakan karyawan untuk membuat keputusan yang tepat saat menangani informasi sensitif.

Terakhir tidak kalah penting, penilaian dan audit keamanan reguler harus dilakukan untuk mengevaluasi efektivitas kontrol keamanan yang ada dan mengidentifikasi area untuk perbaikan. Pemindaian kerentanan dan pengujian penetrasi dapat membantu mengungkap kerentanan tersembunyi dan memvalidasi keseluruhan postur keamanan jaringan.

Dalam implementasi praktik terbaik keamanan IP sangat penting untuk melindungi jaringan dan data sensitif. Dengan mengikuti praktik seperti pembaruan dan tambalan rutin, kontrol akses yang kuat, segmentasi jaringan, enkripsi, pemantauan dan analisis, pencadangan dan pemulihan, kesadaran karyawan, dan penilaian keamanan, organisasi dapat meningkatkan keamanan jaringan IP mereka dan mengurangi potensi ancaman. Mematuhi praktik terbaik ini membantu organisasi mempertahankan postur keamanan proaktif dan bertahan secara efektif dari ancaman dunia maya yang berkembang (Lalit *et al.,* 2022).

9.7 Keamanan IP di Jaringan Nirkabel

Keamanan IP dalam jaringan nirkabel sangat penting untuk memastikan kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui koneksi nirkabel. Jaringan nirkabel, berdasarkan sifatnya, menghadirkan tantangan keamanan yang

unik karena sifat penyiaran sinyal nirkabel dan potensi akses yang tidak sah. Memahami dan menerapkan langkah-langkah keamanan IP dalam jaringan nirkabel sangat penting untuk melindungi informasi sensitif dari penyadapan, akses tidak sah, dan manipulasi data (Mughal, 2022; Yu *et al*., 2022).

Salah satu perhatian utama dalam keamanan jaringan nirkabel adalah perlindungan data selama transmisi. Enkripsi memainkan peran penting dalam mengamankan komunikasi nirkabel. Menerapkan protokol enkripsi yang kuat seperti Wi-Fi *Protected Access* (WPA) atau WPA2 dapat memberikan enkripsi yang kuat untuk koneksi nirkabel, mencegah individu yang tidak sah mencegat dan menguraikan data yang dikirimkan. Enkripsi memastikan bahwa meskipun penyerang berhasil menangkap sinyal nirkabel, informasinya tetap tidak dapat dibaca dan rahasia.
Jaringan nirkabel juga memerlukan mekanisme otentikasi yang efektif untuk memverifikasi identitas perangkat dan pengguna. Menerapkan protokol autentikasi yang kuat, seperti *Extensible Authentication Protocol* (EAP), dikombinasikan dengan metode autentikasi yang aman seperti sertifikat digital atau kunci yang dibagikan sebelumnya, membantu memastikan bahwa hanya perangkat dan pengguna yang diotorisasi yang dapat terhubung ke jaringan nirkabel. Ini mencegah akses tidak sah dan memperkuat keamanan jaringan secara keseluruhan.

Selain enkripsi dan otentikasi, mekanisme kontrol akses memainkan peran penting dalam keamanan jaringan nirkabel. Menerapkan langkah-langkah kontrol akses, seperti segmentasi jaringan nirkabel, aturan firewall, dan LAN virtual (VLAN), membantu mencegah akses tidak sah ke sumber daya sensitif dan membatasi cakupan potensi pelanggaran keamanan. Segmentasi jaringan membantu mengisolasi klien nirkabel, mencegah mereka mengakses komponen jaringan penting atau data sensitif. Firewall dan VLAN semakin meningkatkan kontrol akses dengan

memberlakukan pembatasan arus lalu lintas dan mencegah komunikasi tidak sah antara segmen jaringan yang berbeda.

Pemantauan rutin dan deteksi intrusi sangat penting dalam menjaga keamanan jaringan nirkabel. Sistem deteksi intrusi (IDS) dapat membantu mendeteksi dan memperingatkan administrator terhadap aktivitas yang mencurigakan atau berbahaya di jaringan nirkabel. Selain itu, pemantauan lalu lintas jaringan nirkabel dan analisis log jaringan secara terus-menerus dapat memberikan wawasan tentang potensi insiden atau pelanggaran keamanan, memungkinkan respons dan mitigasi yang tepat waktu.

Penting juga untuk tetap diperbarui dengan tambalan keamanan terbaru dan pembaruan firmware untuk perangkat dan titik akses nirkabel. Produsen sering merilis pembaruan keamanan untuk mengatasi kerentanan dan meningkatkan keamanan jaringan nirkabel. Memperbarui perangkat nirkabel dan titik akses secara teratur membantu mengurangi risiko yang terkait dengan kerentanan yang diketahui dan memperkuat postur keamanan secara keseluruhan (Noviantoro, 2022; Rukmana, 2023).

Pendidikan dan kesadaran pengguna memainkan peran penting dalam keamanan jaringan nirkabel. Pengguna harus dididik tentang praktik terbaik untuk mengamankan perangkat nirkabel mereka, seperti menggunakan kata sandi yang kuat dan unik, memperbarui firmware perangkat secara rutin, dan berhati-hati dalam menghubungkan ke jaringan nirkabel yang tidak tepercaya. Melatih pengguna untuk mengidentifikasi serangan rekayasa sosial, seperti phishing, dapat membantu mencegah potensi pelanggaran keamanan (Atlam *et al.,* 2020).

Urgensi implementasi keamanan IP dalam jaringan nirkabel sangat krusial untuk melindungi kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui koneksi nirkabel. Menerapkan enkripsi yang kuat, otentikasi, mekanisme kontrol akses, pemantauan, dan pendidikan pengguna sangat penting untuk memastikan keamanan jaringan nirkabel. Dengan mengikuti

langkah-langkah ini, organisasi dapat memitigasi risiko yang terkait dengan akses tidak sah, penyadapan, dan manipulasi data, serta mempertahankan kondisi keamanan yang kuat di lingkungan jaringan nirkabel (Román-Castro *et al*., 2018).

9.8 Keamanan IP di *Internet of Things* (IoT)

Keamanan IP di *Internet of Things* (IoT) sangat penting karena proliferasi perangkat yang terhubung dan potensi risiko yang terkait dengan interkonektivitas perangkat ini. Perangkat IoT, seperti peralatan rumah tangga pintar, sensor industri, dan perangkat yang dapat dikenakan, bergantung pada protokol komunikasi berbasis IP untuk bertukar data dan menjalankan berbagai fungsi. Namun, karakteristik unik IoT, termasuk perangkat yang dibatasi sumber daya dan protokol komunikasi yang beragam, menghadirkan tantangan keamanan yang signifikan yang perlu ditangani (Pamarthi & Narmadha, 2022).

Salah satu aspek kunci dari keamanan IP di IoT adalah otentikasi dan kontrol akses. Dengan banyaknya perangkat yang terhubung ke Internet, sangat penting untuk memastikan bahwa hanya perangkat dan pengguna resmi yang dapat mengakses jaringan dan layanan IoT. Mekanisme autentikasi yang kuat, seperti sertifikat digital atau protokol autentikasi aman, harus diterapkan untuk memverifikasi identitas perangkat dan membangun koneksi yang aman. Kebijakan kontrol akses harus diterapkan untuk membatasi akses tidak sah dan membatasi kemampuan komunikasi perangkat IoT hanya untuk fungsi yang diperlukan.

Enkripsi memainkan peran penting dalam mengamankan komunikasi IoT. Karena perangkat IoT menghasilkan dan mengirimkan data dalam jumlah besar, penting untuk melindungi kerahasiaan dan integritas data ini. Algoritme enkripsi yang kuat harus digunakan untuk mengenkripsi data baik saat transit maupun saat istirahat. Enkripsi memastikan bahwa meskipun data

dicegat atau diakses oleh pihak yang tidak berwenang, data tetap tidak dapat dibaca dan aman (Tamsir Ariyadi, 2022).

Selain itu, perangkat IoT sering beroperasi di lingkungan terbatas sumber daya dengan daya pemrosesan dan memori yang terbatas. Oleh karena itu, protokol enkripsi yang ringan dan algoritme kriptografi yang dioptimalkan diperlukan untuk meminimalkan overhead komputasi sambil mempertahankan keamanan yang kuat. Teknik seperti *Elliptic Curve Cryptography* (ECC) dan cipher blok ringan umumnya digunakan di lingkungan IoT untuk mencapai keseimbangan antara keamanan dan efisiensi sumber daya (Yaroub *et al*., n.d.).

Untuk meningkatkan keamanan IP di IoT, sangat penting untuk menerapkan mekanisme pemantauan dan deteksi ancaman yang berkelanjutan. Algoritme deteksi anomali dan sistem deteksi intrusi (IDS) dapat membantu mengidentifikasi potensi pelanggaran keamanan dan perilaku abnormal di jaringan IoT. Sistem ini dapat mendeteksi upaya akses yang tidak sah, pola data yang tidak normal, atau aktivitas berbahaya, sehingga memungkinkan respons yang cepat dan mitigasi potensi ancaman.

Pembaruan dan tambalan rutin sangat penting untuk memastikan keamanan perangkat IoT. Ekosistem IoT sering terdiri dari beragam perangkat dari produsen yang berbeda, masing-masing dengan firmware dan tumpukan perangkat lunaknya sendiri. Produsen (Setiawan *et al.,* 2023) harus menyediakan pembaruan dan tambalan keamanan tepat waktu untuk mengatasi kerentanan yang diketahui dan memperkuat keamanan perangkat IoT. Demikian pula, pengguna harus tetap waspada dan memperbarui perangkat mereka secara teratur untuk melindungi dari ancaman keamanan yang muncul (Lalit *et al.,* 2022).

Mempromosikan kesadaran dan pendidikan keamanan sangat penting dalam ekosistem IoT. Pengguna dan organisasi harus dididik tentang praktik terbaik keamanan IoT, seperti mengubah kata sandi default, menonaktifkan fitur yang tidak perlu,

dan mengonfigurasi perangkat dengan aman. Selain itu, produsen harus memprioritaskan keamanan dalam desain dan pengembangan perangkat IoT, dengan mempertimbangkan praktik pengkodean yang aman, pembaruan firmware yang aman, dan kepatuhan terhadap standar dan pedoman industri.

Dalam hal keamanan IP di *Internet of Things* sangat penting karena penyebaran luas perangkat yang terhubung. Otentikasi dan kontrol akses, enkripsi, protokol ringan, pemantauan dan deteksi ancaman, pembaruan rutin, dan pendidikan keamanan sangat penting untuk membangun keamanan yang kuat di lingkungan IoT. Dengan menangani aspek-aspek ini, organisasi dapat memitigasi risiko yang terkait dengan penerapan IoT, melindungi data sensitif, dan memastikan integritas dan ketersediaan layanan IoT (Rukmana *et al*., 2023). Pendekatan komprehensif dan proaktif terhadap keamanan IP diperlukan untuk membangun kepercayaan dan keyakinan di dunia IoT yang berkembang pesat.

9.9 Kesimpulan

Keamanan IP (*Internet Protocol*) memainkan peran penting dalam keamanan informasi, memastikan kerahasiaan, integritas, dan ketersediaan data yang dikirimkan melalui jaringan IP. Dengan menerapkan langkah-langkah keamanan IP yang kuat, organisasi dapat melindungi informasi sensitif mereka dari akses tidak sah, penyadapan data, perusakan, dan aktivitas berbahaya lainnya.

Sepanjang bab ini, kami menjelajahi berbagai aspek keamanan IP, termasuk dasar-dasar IP, pengalamatan IP, ancaman dan serangan keamanan IP, protokol keamanan IP, dan mekanisme keamanan IP. Kami belajar bahwa memahami dasar-dasar IP sangat penting untuk memahami konsep dasar keamanan IP. Pengalamatan IP memungkinkan identifikasi dan perutean paket data, memfasilitasi komunikasi yang aman di seluruh jaringan.

Namun, dengan manfaat IP muncul berbagai ancaman dan serangan keamanan. Pelaku jahat dapat mengeksploitasi

kerentanan dalam jaringan IP, membahayakan kerahasiaan dan integritas data. Dengan memahami ancaman dan serangan ini, organisasi dapat menerapkan tindakan pencegahan dan pengamanan yang sesuai untuk melindungi jaringan dan data mereka.

Protokol keamanan IP, seperti IPsec dan SSL/TLS, menyediakan kerangka kerja untuk mengamankan komunikasi IP. Protokol ini membangun saluran komunikasi yang aman, mengotentikasi pengguna dan perangkat, dan mengenkripsi data untuk memastikan kerahasiaan. Dengan memanfaatkan protokol ini, organisasi dapat menerapkan enkripsi end-to-end dan melindungi informasi sensitif dari akses dan intersepsi yang tidak sah.

Selain itu, mekanisme keamanan IP, seperti enkripsi, otentikasi, kontrol akses, deteksi dan pencegahan intrusi, segmentasi jaringan, dan manajemen kunci aman, berkontribusi pada kerangka kerja keamanan IP yang kuat. Mekanisme ini secara kolektif memberikan perlindungan komprehensif terhadap risiko keamanan dan membantu menjaga integritas dan ketersediaan jaringan IP.

Penting bagi organisasi untuk mengikuti praktik terbaik keamanan IP, termasuk pembaruan dan tambalan rutin, kontrol akses yang kuat, segmentasi jaringan, enkripsi, pemantauan dan analisis, pencadangan dan pemulihan, kesadaran karyawan, dan penilaian keamanan. Dengan mengikuti praktik ini, organisasi dapat meningkatkan keamanan jaringan IP mereka, mengurangi potensi ancaman, dan menjaga postur keamanan proaktif.

Di dunia yang saling terhubung saat ini, di mana jaringan IP membentuk tulang punggung komunikasi dan pertukaran informasi, keamanan IP merupakan aspek mendasar dari keamanan informasi. Organisasi harus memprioritaskan keamanan IP untuk melindungi data penting mereka, menjaga kepercayaan

pemangku kepentingan mereka, dan melindungi dari ancaman dunia maya yang berkembang.

Dengan tetap mendapatkan informasi tentang tren dan kemajuan terbaru dalam keamanan IP, terus memperbarui langkah-langkah keamanan, dan mendorong budaya kesadaran keamanan, organisasi dapat membangun jaringan IP yang tangguh dan aman. Dengan fondasi yang kuat dalam keamanan IP, organisasi dapat dengan yakin menavigasi lanskap digital, memanfaatkan kekuatan jaringan IP, dan melindungi aset informasi mereka yang berharga.

DAFTAR PUSTAKA

Akter, H., Jahan, S., Saha, S., Faisal, R. H., & Islam, S. 2022. Evaluating performances of VPN tunneling protocols based on application service requirements. *Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021*, 433–444.

Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. 2020. Security, cybercrime and digital forensics for IoT. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, 551–577.

Aydos, M., Savas, E., & Koc, C. K. 1999. Implementing network security protocols based on elliptic curve cryptography. *Proceedings of the Fourth Symposium on Computer Networks*, 130–139.

Choubey, D. K., Shukla, V., Soni, V., Kumar, J., & Dheer, D. K. 2022. A review on IoT architectures, protocols, security, and applications. *Industrial Internet of Things*, 225–242.

Dara, Y. C., Hariadi, F., & Lede, P. A. R. L. 2023. Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp Snooping Dan Switch Port Security. *JURNAL TEKNIK INFORMATIKA INOVATIF WIRA WACANA*, *1*(3), 187–196.

DeNardis, L. 2022. Quantum Internet Protocols. *Available at SSRN 4182865*.

Forouzan, B. A., & Mukhopadhyay, D. 2015. *Cryptography and network security* (Vol. 12). Mc Graw Hill Education (India) Private Limited New York, NY, USA:

Foruzan, B. 2007. Cryptography and network security. *Policy*, *3*, 4.

Hananto, A. L. 2023. *Tata Kelola Keamanan Sistem Informasi*. Media Sains Indonesia.

Harto, B., Saymsu, Y. L., Rukmana, A. Y., Komalasari, R., & Dwijayanti, A. 2022. Bibliometric Analysis of Transforming Leadership Education with Artificial Intelligence. In *1st*

Virtual Workshop on Writing Scientific Article for International Publication Indexed SCOPUS (pp. 385–390). Sciendo. https://doi.org/10.2478/9788366675827-067

Hassan, H. A. 2022. Review Vehicular Ad hoc Networks Security Challenges and Future Technology. *Wasit Journal of Computer and Mathematics Science*, *1*(3).

Herman, H., Umar, R., & Marsaid, A. P. 2023. Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration. *JURIKOM (Jurnal Riset Komputer)*, *10*(1), 317–329.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. 2022. *Cybercrime and digital forensics: An introduction*. Routledge.

Indrawan, A. J. (n.d.). *IoT dan Blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi*.

Jamaluddin, J., & Siringoringo, R. 2023. PENGONTROLAN KEAMANAN SISTEM KOMPUTER CLIENT DARI SERANGAN HACKER DAN VIRUS KOMPUTER SECARA JARAK JAUH (REMOTE SERVER) DENGAN MENGGUNAKAN SSH. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, *7*(1), 123–127.

Kaeo, M. 2004. *Designing network security*. Cisco Press.

Kizza, J. M. 2005. *Computer network security*. Springer.

Lalit, M., Chawla, S. K., Rana, A. K., Nisar, K., Soomro, T. R., & Khan, M. A. 2022. IoT networks: Security vulnerabilities of application layer protocols. *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 1–5.

Marin, G. A. 2005. Network security basics. *IEEE Security & Privacy*, *3*(6), 68–72.

Mughal, A. A. 2022. Well-Architected Wireless Network Security. *Journal of Humanities and Applied Science Research*, *5*(1), 32–42.

Munawar, Z., & Putri, N. I. 2020. Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14–20.

Noviantoro, G. Y. 2022) Analisa Perbandingan Antar Kualitas Jaringan VPN IP Security Dan ZRTP Pada Voice Over Internet Protocol. *Jurnal Teknologi Pintar*, *2*(3).

Pamarthi, S., & Narmadha, R. 2022. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, *10*(4), 482–506.

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. 2003. Analyzing the energy consumption of security protocols. *Proceedings of the 2003 International Symposium on Low Power Electronics and Design*, 30–35.

Puspita, H., Mulyana, A., Putro, H. P., Sihombing, F. A. H., Ikhram, F., Sutjiningtyas, S., Utomo, S., Andriani, A. D., Pratiwi, V., & Friadi, J. 2022. *Pengantar Teknologi Informasi*. Haura Utama.

Rahardjo, B. 2005. Keamanan sistem informasi berbasis internet. *Bandung: PT. Insan Indonesia*.

Román-Castro, R., López, J., & Gritzalis, S. 2018. Evolution and trends in IoT security. *Computer*, *51*(7), 16–25.

Rukmana, A. Y. 2023. BAB 3 TEKNOLOGI DIGITAL. *Digital Marketing Dan E-Commerce*, 27.

Rukmana, A. Y., Zebua, R. S. Y., Aryanto, D., Nur'Aini, I., Ardiansyah, W., Adhicandra, I., & Setiawan, Z. 2023. *DUNIA MULTIMEDIA: Pengenalan dan Penerapannya*. PT. Sonpedia Publishing Indonesia.

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. 2022. Internet of Things: Security and Solutions Survey. *Sensors*, *22*(19), 7433.

Sen, J. 2013. *Theory and practice of cryptography and network security protocols and technologies*. BoD–Books on Demand.

Setiawan, Z., Jauhar, N., Putera, D. A., Santosa, A. D., Fenanlampir, K., Sembel, H. F., Harto, B., Roza, T. A., Dermawan, A. A., & Rukmana, A. Y. 2023. *Kewirausahaan Digital*. Global Eksekutif Teknologi.

Taghizad-Tavana, K., Ghanbari-Ghalehjoughi, M., Razzaghi-Asl, N., Nojavan, S., & Alizadeh, A. ad. 2022. An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges. *Sustainability*, *14*(23), 15938.

Tamsir Ariyadi, T. 2022. Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security. *Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security*.

VARGA, M., & KUJUNDZIC, M. 2022. Innovative Technologies of Web Services and Security Protocols. *Co-Editors*, 35.

Wakil, A., Cahyani, R. R., Harto, B., Latif, A. S., Hidayatullah, D., Simanjuntak, P., Rukmana, A. Y., & Sihombing, F. A. H. 2022. *Transformasi Digital Dalam Dunia Bisnis*. Global Eksekutif Teknologi.

Yanto Rukmana, A., Harto, B., & Gunawan, H. 2021. Analisis Urgensi Kewirausahaan Berbasis Teknologi (Technopreneurship) dan Peranan Society 5.0 dalam Perspektif Ilmu Pendidikan Kewirausahaan. In *Jurnal Sains Manajemen & Akuntansi)* (Vol. 13, Issue 1).

Yaroub, H. M., Naif, A. P. D. J. R., & Hasan, S. M. (n.d.). *Security Challenges And Security Protocols For Wireless Sensor Networks: A Review*.

Yu, J., Ye, X., & Li, H. 2022. A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Future Generation Computer Systems*, *129*, 399–406.

BAB 10
FIREWALL

Oleh Suwito Pomalingo

10.1 Pendahuluan

Keamanan siber adalah aspek yang sangat penting dalam era digital saat ini. Salah satu komponen penting dari sistem keamanan siber adalah firewall. Firewall berfungsi sebagai pertahanan pertama dalam melindungi sistem dan jaringan dari serangan yang berasal dari luar. Bab ini dirancang untuk memberikan pemahaman yang mendalam tentang firewall: bagaimana mereka bekerja, bagaimana mengkonfigurasikannya, dan bagaimana menggunakan firewall untuk mempertahankan sistem dan jaringan.

Firewall adalah sistem yang dirancang untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi. Dalam hal ini, firewall dapat dianggap sebagai penjaga keamanan digital, yang bertugas memeriksa data yang masuk dan keluar dari jaringan dan memblokir atau membolehkan data tersebut berdasarkan serangkaian aturan keamanan yang telah ditentukan.

Pada bagian ini, kita akan membahas berbagai jenis firewall, termasuk firewall berbasis perangkat keras, firewall berbasis perangkat lunak, dan firewall berbasis cloud. Kita juga akan membahas bagaimana firewall dapat digunakan dalam berbagai skenario, mulai dari melindungi jaringan rumah hingga melindungi infrastruktur IT perusahaan besar.

Pengetahuan tentang firewall sangat penting untuk siapa saja yang berkecimpung dalam bidang IT, baik sebagai profesional IT, pelajar, atau bahkan pengguna rumahan. Dengan pengetahuan yang tepat, kita dapat membuat keputusan yang lebih baik tentang

bagaimana melindungi data dan informasi penting kita dari berbagai ancaman yang ada di dunia siber.

10.1.1 Definisi dan fungsi *Firewall*

Firewall adalah suatu sistem yang bertujuan untuk melindungi jaringan komputer dari serangan yang datang dari luar jaringan (Ferguson and Huston, 1998). Dalam bahasa yang lebih sederhana, firewall bisa dianalogikan sebagai penjaga pintu yang memiliki tugas untuk memeriksa semua data yang masuk dan keluar melalui jaringan tersebut.

Firewall biasanya diterapkan sebagai perangkat keras (*hardware*) atau perangkat lunak (*software*), atau kombinasi dari keduanya. Bisa juga berupa layanan berbasis cloud yang dirancang untuk melindungi infrastruktur dan data yang ada di cloud (Mirkovic and Reiher, 2004)

Fungsi utama dari firewall adalah untuk melindungi sistem atau jaringan komputer dari ancaman dan serangan dari dunia luar. Firewall memeriksa semua data yang masuk dan keluar dari jaringan berdasarkan serangkaian aturan yang telah ditentukan, dan kemudian memutuskan untuk memblokir atau mengizinkan data tersebut berdasarkan aturan tersebut (Zwicky, Cooper and Chapman, 2000).

Firewall juga berfungsi untuk memisahkan jaringan internal dari jaringan eksternal, seperti internet, dan menyediakan kontrol yang ketat atas apa yang boleh masuk dan keluar dari jaringan tersebut. Dengan demikian, firewall memainkan peran penting dalam menjaga integritas dan kerahasiaan data di dalam jaringan (Zeltser *et al.*, 2002).

Selain itu, firewall juga dapat digunakan untuk mencatat aktivitas jaringan, yang dapat digunakan untuk mendeteksi adanya usaha penyerangan atau penyalahgunaan jaringan (Stallings and Brown, 2018).

10.1.2 Sejarah dan evolusi Firewall

Sejarah penggunaan firewall dalam teknologi informasi dimulai sejak tahun 1980-an. Pada masa itu, firewall pertama kali diperkenalkan sebagai sebuah sistem untuk memisahkan jaringan internal sebuah organisasi dari jaringan eksternal seperti internet (Cheswick *et al.*, 2003). Tujuannya adalah untuk melindungi data dan sistem yang ada di dalam jaringan internal dari serangan yang berasal dari luar.

Firewall pertama yang dikenal adalah jenis firewall berbasis paket atau *packet filtering firewall*. Firewall jenis ini bekerja dengan memeriksa setiap paket data yang masuk dan keluar dari jaringan dan memutuskan untuk memblokir atau mengizinkan paket tersebut berdasarkan alamat IP dan port tujuan (Chapman, 1992). Namun, firewall jenis ini memiliki kelemahan yaitu tidak mampu untuk memahami konteks dari data yang dikirimkan.

Selanjutnya, pada tahun 1990-an, diperkenalkan firewall generasi kedua yang dikenal sebagai firewall berbasis state (*stateful firewall* dan *stateless* f*irewall*). Firewall jenis ini mampu melacak koneksi dan menyimpan informasi tentang koneksi tersebut dalam tabel status, yang memungkinkan firewall untuk memahami konteks dari data yang dikirimkan (Eddy, 2007).

Pada awal tahun 2000-an, muncul firewall generasi ketiga yang dikenal sebagai firewall aplikasi atau *application firewall*. Firewall jenis ini mampu memeriksa dan memfilter data hingga ke tingkat aplikasi, yang memungkinkan kontrol yang lebih ketat atas jenis data yang boleh masuk dan keluar dari jaringan (Stallings and Brown, 2018).

Saat ini, dengan semakin kompleksnya ancaman keamanan, telah muncul berbagai jenis firewall canggih seperti firewall berbasis *cloud* dan *firewall next-generation* (NGFW) yang mampu melakukan fungsi-fungsi lebih lanjut seperti identifikasi aplikasi, pencegahan intrusi, dan perlindungan terhadap ancaman lanjutan lainnya (Cisco, 2021).

10.1.3 Jenis-jenis *Firewall*

Firewall dapat diklasifikasikan menjadi beberapa jenis berdasarkan cara kerja dan fungsionalitasnya. Berikut ini adalah beberapa jenis firewall yang paling umum digunakan, beserta penjelasan perbedaannya.

1. Firewall Berbasis Paket (*Packet Filtering Firewall*): Firewall jenis ini merupakan jenis firewall yang paling dasar. Firewall ini bekerja dengan memeriksa setiap paket data yang masuk dan keluar dari jaringan dan memutuskan untuk memblokir atau mengizinkan paket tersebut berdasarkan alamat IP dan port tujuan. Sementara firewall berbasis paket cepat dan efisien, mereka tidak mampu memahami konteks atau 'state' dari koneksi, yang berarti mereka kurang mampu melindungi terhadap serangan yang lebih canggih.
2. Firewall Berbasis State: Firewall jenis ini lebih canggih dibandingkan dengan firewall berbasis paket. Firewall berbasis state mampu melacak koneksi dan menyimpan informasi tentang koneksi tersebut dalam tabel status. Hal ini memungkinkan firewall untuk memahami konteks dari data yang dikirimkan, sehingga dapat memberikan perlindungan yang lebih baik terhadap serangan yang memanfaatkan koneksi yang ada. Namun, firewall jenis ini membutuhkan lebih banyak sumber daya komputasi dibandingkan dengan firewall berbasis paket.
3. Firewall Aplikasi: Firewall jenis ini beroperasi pada lapisan aplikasi dari model referensi OSI dan mampu memeriksa dan memfilter data hingga ke tingkat aplikasi. Hal ini memungkinkan kontrol yang lebih ketat atas jenis data yang boleh masuk dan keluar dari jaringan. Selain itu, firewall aplikasi juga mampu melindungi terhadap serangan yang dirancang untuk mengeksploitasi kerentanan pada aplikasi tertentu.

4. Firewall Berbasis Proxy: Firewall berbasis proxy bertindak sebagai perantara antara sumber dan tujuan lalu lintas jaringan. Firewall ini memeriksa dan menyaring semua lalu lintas yang lewat, dan juga dapat menyediakan fungsionalitas tambahan seperti caching dan kontrol akses yang lebih granular. Kelemahan dari firewall jenis ini adalah mereka dapat menyebabkan penundaan dalam lalu lintas jaringan karena proses perantara yang harus dilalui.
5. Firewall Generasi Selanjutnya (*Next Generation Firewall - NGFW*): Firewall generasi selanjutnya adalah jenis firewall yang paling canggih dan dilengkapi dengan berbagai fungsi tambahan seperti identifikasi aplikasi, pencegahan intrusi, dan perlindungan terhadap ancaman lanjutan lainnya. Kelebihan utama dari firewall jenis ini adalah kemampuannya untuk memberikan perlindungan yang komprehensif terhadap berbagai jenis ancaman, meskipun dengan biaya penggunaan sumber daya yang lebih besar dan kompleksitas yang lebih tinggi dibandingkan dengan jenis firewall lainnya.

Memilih jenis firewall yang tepat bergantung pada kebutuhan spesifik dari jaringan atau sistem yang ingin Anda lindungi. Berikut ini adalah beberapa pertimbangan yang mungkin dapat membantu Anda dalam membuat keputusan tersebut:

1. Ukuran dan Jenis Jaringan: Jika Anda mengelola jaringan kecil dengan lalu lintas data yang relatif sedikit, firewall berbasis paket mungkin sudah cukup. Namun, untuk jaringan yang lebih besar dan kompleks, Anda mungkin membutuhkan firewall berbasis state atau bahkan firewall generasi selanjutnya.
2. Kebutuhan Keamanan: Jika data yang Anda kelola sangat sensitif dan berharga, atau jika Anda beroperasi dalam lingkungan yang sering menjadi target serangan, maka

Anda mungkin perlu menggunakan firewall dengan tingkat perlindungan yang lebih tinggi, seperti firewall aplikasi atau firewall generasi selanjutnya.

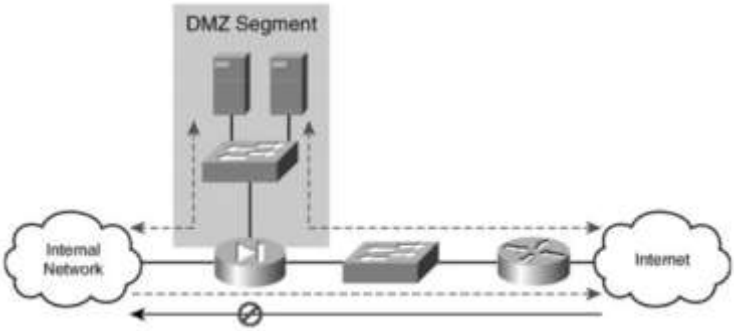
3. Sumber Daya dan Anggaran: Firewall yang lebih canggih biasanya membutuhkan lebih banyak sumber daya komputasi dan mungkin lebih mahal. Jadi, Anda perlu mempertimbangkan ketersediaan dan anggaran Anda sebelum memilih jenis firewall yang akan digunakan.

Sangat penting untuk dicatat bahwa tidak ada satu jenis firewall yang dapat memberikan perlindungan 100% terhadap semua jenis ancaman. Oleh karena itu, firewall biasanya digunakan sebagai bagian dari strategi keamanan yang lebih luas yang mencakup berbagai jenis kontrol keamanan lainnya, seperti sistem deteksi intrusi, enkripsi, otentikasi pengguna, dan lainnya.

10.1.4 Arsitektur Firewall

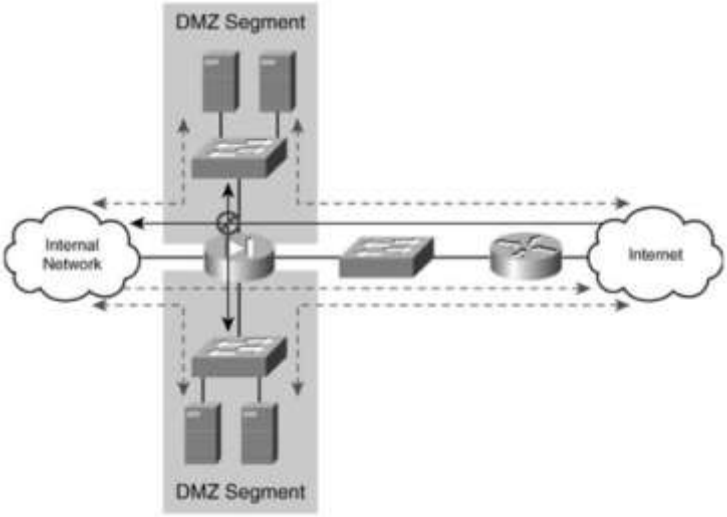
Arsitektur firewall merujuk kepada bagaimana firewall ditempatkan dan diatur dalam jaringan untuk memberikan tingkat keamanan yang optimal. Berikut adalah beberapa arsitektur firewall yang umum digunakan:

1. Arsitektur Firewall Tunggal: Dalam arsitektur ini, satu firewall ditempatkan di antara jaringan internal dan jaringan eksternal (seperti internet). Semua lalu lintas yang masuk dan keluar dari jaringan harus melewati firewall ini, yang memeriksa dan memfilter lalu lintas berdasarkan aturan yang ditetapkan.



Gambar 10.1. Arsitektur Firewall Tunggal
(Sumber : flylib.com)

2. Arsitektur Dual Firewall atau DMZ (*Demilitarized Zone*): Dalam arsitektur ini, dua firewall digunakan. Salah satu firewall ditempatkan di antara jaringan internal dan DMZ, dan firewall lainnya ditempatkan di antara DMZ dan jaringan eksternal. DMZ biasanya berisi server yang perlu diakses dari internet, seperti server web atau server email. Dengan cara ini, bahkan jika server di DMZ dikompromikan, penyerang masih harus melewati firewall lainnya untuk mengakses jaringan internal.
3. Arsitektur Multi-Layer Firewall: Dalam arsitektur ini, beberapa firewall ditempatkan di berbagai titik dalam jaringan untuk memberikan lapisan keamanan tambahan. Misalnya, Anda mungkin memiliki firewall berbasis paket di tepi jaringan untuk memblokir lalu lintas yang jelas-jelas berbahaya, dan kemudian memiliki firewall generasi selanjutnya atau firewall aplikasi lebih dalam dalam jaringan untuk memberikan inspeksi lalu lintas yang lebih rinci.



Gambar 10.2. Arsitektur Dual Firewall
(Sumber : flylib.com)

Arsitektur yang dipilih untuk suatu jaringan akan sangat bergantung pada ukuran jaringan, jenis lalu lintas yang diharapkan, dan tingkat keamanan yang diperlukan. Penting untuk mempertimbangkan faktor-faktor ini secara hati-hati saat merancang arsitektur firewall untuk jaringan Anda.

10.2 Cara Kerja Firewall

Dalam menjalankan fungsinya, firewall bekerja berdasarkan konsep inspeksi paket dan aturan yang ditetapkan sebelumnya. Saat data dikirimkan melalui jaringan, data tersebut dibagi menjadi paket. Firewall pertama-tama akan menerima paket data tersebut dan memeriksa informasi yang ada di dalamnya, seperti alamat IP sumber dan tujuan, port, protokol, dan lain sebagainya. Proses ini dikenal dengan istilah inspeksi paket. Berikut penjelasan bagaimana cara kerja firewall.

10.2.1 Proses pengambilan keputusan Firewall

Firewall berperan penting dalam pengendalian akses dan lalu lintas dalam suatu jaringan. Ia melakukan hal ini melalui proses pengambilan keputusan yang terstruktur dan terdefinisi dengan baik. Setiap kali ada paket data yang mencoba melewati firewall, baik masuk atau keluar dari jaringan, firewall akan memulai proses pengambilan keputusan.

Proses ini dimulai dengan inspeksi paket, di mana firewall memeriksa informasi yang terdapat dalam paket data. Informasi ini meliputi, tetapi tidak terbatas pada, alamat IP sumber dan tujuan, nomor port, dan jenis protokol yang digunakan. Setiap detail ini dianalisis dan dinilai oleh firewall.

Setelah inspeksi paket, firewall akan membandingkan informasi yang ada dalam paket dengan serangkaian aturan atau kebijakan yang telah ditetapkan. Aturan atau kebijakan ini didefinisikan oleh administrator jaringan dan mencakup berbagai parameter, seperti alamat IP yang diizinkan, port yang diblokir, dan jenis protokol yang diperbolehkan.

Berdasarkan penilaian terhadap aturan tersebut, firewall akan memutuskan apakah paket data tersebut akan diblokir atau diizinkan untuk melanjutkan perjalanan menuju tujuan aslinya. Jika paket data memenuhi aturan yang membuatnya harus diblokir, maka firewall akan mencegah paket tersebut untuk melanjutkan perjalanan. Sebaliknya, jika paket data tidak memenuhi aturan pemblokiran, paket tersebut akan diizinkan untuk melanjutkan perjalanan.

Pada akhirnya, cara kerja firewall adalah sebuah proses selektif yang menentukan paket data mana yang dapat melintasi jaringan dan mana yang harus diblokir. Meski demikian, penting untuk diingat bahwa firewall bukanlah solusi keamanan yang lengkap. Untuk perlindungan yang optimal, firewall sebaiknya digunakan sebagai bagian dari strategi keamanan yang lebih luas yang mencakup berbagai tipe pengendalian keamanan lainnya.

Setelah memutuskan apakah akan mengizinkan atau memblokir paket, firewall juga bertugas mencatat kejadian tersebut. Beberapa firewall dilengkapi dengan fitur logging dan pelaporan, yang memungkinkan administrator jaringan untuk memantau aktivitas dan kejadian dalam jaringan. Informasi ini sangat berharga untuk analisis keamanan jaringan, memungkinkan identifikasi pola serangan atau aktivitas mencurigakan.

Fitur-fitur ini menjadikan firewall sebagai alat yang sangat penting dalam menjaga keamanan jaringan. Dengan memantau dan mengendalikan lalu lintas jaringan, firewall mampu mencegah ancaman eksternal yang berpotensi merusak sistem atau mencuri data. Dalam banyak kasus, firewall menjadi lapisan pertama dan sangat penting dalam pertahanan suatu jaringan.

10.2.2 Mengenali algoritma dan aturan Firewall

Untuk dapat bekerja dengan efektif, firewall mengandalkan suatu serangkaian aturan dan algoritma yang telah ditetapkan oleh administrator jaringan. Algoritma dan aturan ini menentukan bagaimana firewall memutuskan mana lalu lintas jaringan yang harus diblokir dan mana yang harus diizinkan.

Aturan firewall biasanya ditentukan berdasarkan serangkaian parameter yang dapat mencakup alamat IP sumber dan tujuan, nomor port, jenis protokol, dan bahkan waktu transaksi. Misalnya, aturan firewall mungkin menentukan bahwa semua lalu lintas yang datang dari alamat IP tertentu harus diblokir, atau semua lalu lintas yang menuju ke port tertentu harus diizinkan. Aturan-aturan ini biasanya ditentukan oleh administrator jaringan berdasarkan kebutuhan dan kebijakan keamanan perusahaan.

Algoritma yang digunakan oleh firewall berfungsi untuk memproses dan mengevaluasi aturan-aturan tersebut. Ketika paket data mencoba melewati firewall, algoritma ini akan memeriksa setiap detail dari paket tersebut dan membandingkannya dengan

aturan yang ada. Berdasarkan hasil dari perbandingan ini, algoritma kemudian akan memutuskan apakah paket tersebut harus diblokir atau diizinkan melewati firewall.

Selain itu, beberapa firewall canggih juga menggunakan algoritma untuk melakukan tugas seperti inspeksi isi paket (packet inspection) dan deteksi serangan berbasis aplikasi. Algoritma ini memungkinkan firewall untuk mengidentifikasi dan memblokir ancaman yang lebih kompleks, seperti serangan zero-day atau serangan yang mengeksploitasi kerentanan dalam aplikasi spesifik.

Memahami algoritma dan aturan firewall adalah penting dalam pengaturan dan manajemen keamanan jaringan. Dengan pengetahuan yang tepat, administrator jaringan dapat mengkonfigurasi firewall untuk memberikan tingkat perlindungan yang paling optimal bagi jaringannya.

Dalam pengaturan firewall, ada dua prinsip dasar yang biasa digunakan, yaitu "*default deny*" dan "*default permit*". Kedua prinsip ini merujuk pada bagaimana firewall akan bereaksi terhadap lalu lintas jaringan yang tidak secara spesifik dicakup oleh aturan yang telah ditetapkan.

1. Default Deny. Prinsip ini berarti bahwa firewall secara default akan menolak semua lalu lintas jaringan, kecuali jika ada aturan spesifik yang memperbolehkannya. Dalam skenario ini, administrator jaringan harus secara eksplisit mendefinisikan jenis lalu lintas apa saja yang diizinkan melalui firewall. Semua lalu lintas lainnya, yang tidak dicakup oleh aturan-aturan tersebut, akan secara otomatis diblokir. Prinsip ini cenderung lebih aman, karena hanya lalu lintas yang dikenali dan dianggap aman yang diizinkan, namun dapat menjadi sangat kompleks dan memerlukan manajemen yang intensif.
2. Default Permit. Prinsip ini berarti bahwa firewall secara default akan mengizinkan semua lalu lintas jaringan, kecuali jika ada aturan spesifik yang melarangnya. Dalam

skenario ini, administrator jaringan harus mendefinisikan jenis lalu lintas apa saja yang tidak diizinkan. Semua lalu lintas lainnya, yang tidak dicakup oleh aturan-aturan tersebut, akan secara otomatis diizinkan. Meski prinsip ini lebih sederhana dan memerlukan manajemen yang kurang intensif, ia juga lebih rentan terhadap ancaman, karena secara default semua lalu lintas diizinkan, termasuk yang berpotensi berbahaya.

Dalam membuat algoritma dan aturan firewall, sangat penting untuk menentukan prinsip mana yang akan digunakan. Pilihan antara "default deny" dan "default permit" akan sangat mempengaruhi keamanan jaringan, efisiensi manajemen firewall, dan kemampuan jaringan untuk mendukung operasional bisnis. Keputusan ini harus didasarkan pada penilaian risiko dan kebutuhan bisnis, serta pertimbangan ketersediaan sumber daya untuk manajemen firewall. Biasanya, pendekatan "default deny" lebih disukai dalam pengaturan keamanan jaringan karena lebih mampu mencegah ancaman tak terduga.

10.3 Konfigurasi dan Pengaturan Firewall

Dalam menjalankan fungsinya, firewall memerlukan konfigurasi dan pengaturan yang tepat. Langkah-langkah dalam konfigurasi dan pengaturan firewall dapat beragam tergantung pada jenis dan model firewall yang digunakan, namun beberapa prinsip umum berlaku.

Pertama-tama, konfigurasi firewall dimulai dengan menentukan aturan-aturan yang akan digunakan. Aturan-aturan ini akan mendefinisikan jenis lalu lintas jaringan yang diizinkan dan yang tidak diizinkan. Misalnya, aturan mungkin menentukan bahwa semua lalu lintas dari alamat IP tertentu harus diblokir, atau bahwa semua lalu lintas yang menuju ke port tertentu harus

diizinkan. Aturan-aturan ini harus disesuaikan dengan kebutuhan dan kebijakan keamanan organisasi.

Setelah aturan ditentukan, mereka harus diterapkan dalam konfigurasi firewall. Cara spesifik untuk melakukan ini akan bervariasi tergantung pada perangkat atau perangkat lunak firewall yang digunakan, tetapi biasanya melibatkan memasukkan aturan-aturan ke dalam antarmuka konfigurasi firewall.

Selanjutnya, firewall harus diatur untuk log aktivitas dan memantau lalu lintas jaringan. Fungsi ini memungkinkan administrator jaringan untuk melacak aktivitas di jaringan dan mengidentifikasi potensi ancaman atau masalah. Fungsi ini biasanya dapat diatur melalui antarmuka konfigurasi firewall.

Akhirnya, setelah firewall dikonfigurasi, penting untuk melakukan pengujian untuk memastikan bahwa firewall berfungsi dengan benar dan sesuai dengan kebutuhan organisasi. Ini dapat melibatkan pengujian penembusan, di mana berbagai upaya dilakukan untuk meretas jaringan dan mencari celah dalam pertahanan firewall.

Konfigurasi dan pengaturan firewall adalah proses yang memerlukan pengetahuan teknis dan pemahaman mendalam tentang jaringan dan keamanan informasi. Untuk mendapatkan hasil terbaik, disarankan untuk berkonsultasi dengan ahli keamanan jaringan atau perusahaan yang berpengalaman dalam konfigurasi dan manajemen firewall.

Selain itu, penting untuk memperhatikan bahwa konfigurasi firewall harus dilakukan dengan hati-hati dan akurat. Kesalahan kecil dalam aturan atau pengaturan dapat menyebabkan celah keamanan yang dapat dimanfaatkan oleh penyerang. Oleh karena itu, sangat penting untuk selalu melakukan pengecekan dan verifikasi setelah melakukan perubahan pada konfigurasi firewall.

10.3.1 Bagaimana menetapkan aturan pada Firewall

Menetapkan aturan pada firewall adalah langkah krusial dalam proses konfigurasi firewall. Aturan-aturan ini berfungsi

sebagai pedoman bagi firewall dalam mengizinkan atau memblokir lalu lintas jaringan. Proses ini melibatkan pemahaman mendalam tentang kebutuhan jaringan dan kebijakan keamanan organisasi.
Sebelum memulai, penting untuk memiliki pemahaman yang jelas tentang struktur dan kebutuhan jaringan. Ini melibatkan pemahaman tentang sistem mana yang harus diakses, siapa saja yang perlu mengakses sistem tersebut, dan bagaimana pola lalu lintas jaringan normal. Dengan pemahaman ini, Anda dapat menentukan aturan yang paling sesuai untuk memenuhi kebutuhan tersebut.

Setelah itu, Anda dapat mulai menetapkan aturan pada firewall. Untuk melakukan ini, Anda perlu mengakses antarmuka konfigurasi firewall. Setiap firewall mungkin memiliki antarmuka yang sedikit berbeda, tetapi umumnya, Anda akan perlu memasukkan parameter seperti alamat IP sumber dan tujuan, port, dan protokol yang digunakan.

Dalam menetapkan aturan, prinsip "*default deny*" atau "*default permit*" bisa dijadikan panduan. Jika Anda mengikuti prinsip "*default deny*", Anda perlu menetapkan aturan yang secara spesifik memperbolehkan lalu lintas tertentu, dan semua lalu lintas lainnya akan diblokir. Sebaliknya, jika Anda mengikuti prinsip "default permit", Anda perlu menetapkan aturan yang secara spesifik melarang lalu lintas tertentu, dan semua lalu lintas lainnya akan diizinkan.

Setelah aturan ditetapkan dan diterapkan, sangat penting untuk melakukan pengetesan untuk memastikan bahwa aturan bekerja sesuai yang diharapkan. Ini juga merupakan kesempatan untuk mengevaluasi apakah aturan tersebut telah mencakup semua kemungkinan skenario atau apakah ada yang belum ditangani.

Secara keseluruhan, menetapkan aturan pada firewall adalah proses yang membutuhkan pemikiran strategis dan pemahaman teknis. Namun, dengan perencanaan dan pelaksanaan

yang tepat, Anda dapat membuat firewall yang efektif dalam melindungi jaringan Anda.

10.3.2 Kebijakan keamanan dan penerapannya dalam Firewall

Firewall dikonfigurasi dengan menggunakan serangkaian aturan, atau yang biasa disebut "*rules*", yang menentukan jenis lalu lintas mana yang diperkenankan atau diblokir. Biasanya, aturan-aturan ini berdasar pada parameter-parameter seperti alamat IP, port, dan protokol. Inilah beberapa contoh dari aturan firewall:

1. Memblokir lalu lintas dari alamat IP tertentu.
   Jika ada alamat IP spesifik yang dikenal mencoba melakukan serangan atau aktivitas yang mencurigakan, kita dapat menciptakan aturan yang akan menyekat seluruh lalu lintas dari alamat IP tersebut. Sebagai contoh, aturan bisa seperti ini: "DENY FROM IP 192.168.1.100".
2. Membatasi akses ke port tertentu.
   Kita bisa mengatur aturan untuk membatasi akses ke port spesifik guna mencegah akses yang tidak sah. Misalnya, kita dapat mengatur aturan yang hanya memperbolehkan alamat IP tertentu untuk mengakses port 22 (SSH): "ALLOW TCP FROM IP 192.168.1.1 TO ANY PORT 22".
3. Memblokir protokol tertentu.
   Kita dapat menciptakan aturan yang menyekat protokol spesifik jika protokol tersebut tidak diperlukan atau berpotensi berisiko. Misalnya, menciptakan aturan untuk menyekat semua lalu lintas ICMP untuk mencegah serangan ping: "DENY ICMP FROM ANY TO ANY".
4. Membatasi akses ke situs web spesifik.
   Di dalam organisasi atau tempat kerja, sering kali diperlukan aturan yang memblokir akses ke situs web spesifik. Sebagai contoh, kita bisa menciptakan aturan

untuk menyekat akses ke situs web media sosial selama jam kerja: "DENY TCP FROM ANY TO www.facebook.com".

Berikut adalah contoh sederhana dari sebuah tabel aturan firewall. Tabel ini menunjukkan aturan yang bisa diimplementasikan di dalam sebuah firewall untuk mengendalikan lalu lintas jaringan berdasarkan protokol, alamat IP sumber, alamat IP tujuan, port sumber, dan port tujuan.

Tabel 10.1. Tabel Aturan Firewall

NO	Protocol	Alamat IP Sumber	Port Sumber	Alamat IP Tujuan	Port Tujuan	Aksi
1	TCP	192.168.1.100	Any	192.168.1.1	22	Allow
2	TCP	Any	Any	192.168.1.2	80	Allow
3	UDP	Any	Any	192.168.1.2	53	Allow
4	TCP	192.168.1.100	Any	Any	Any	Deny
5	ICMP	Any	Any	Any	Any	Deny

10.4 Manajemen dan Pemeliharaan Firewall

Manajemen dan pemeliharaan firewall merupakan elemen penting dalam menjaga keamanan jaringan sebuah organisasi. Tugas ini bukan hanya melibatkan penyiapan dan konfigurasi awal, tetapi juga monitoring, pembaruan, peningkatan, dan penyesuaian aturan berdasarkan perubahan lalu lintas jaringan dan ancaman keamanan baru.

Pada tahap manajemen, firewall harus diatur dengan tepat untuk menghadapi ancaman yang ada serta memenuhi kebutuhan spesifik jaringan dan organisasi. Ini mencakup penentuan aturan firewall, pemilihan jenis firewall, dan pengaturan konfigurasi lainnya. Selain itu, akses ke manajemen firewall juga harus dikelola dengan cermat untuk mencegah perubahan yang tidak sah atau malapetaka keamanan lainnya.

Monitoring atau pemantauan adalah bagian integral dari manajemen firewall. Dengan pemantauan yang tepat, Anda dapat mengidentifikasi adanya aktivitas mencurigakan atau tidak normal dalam jaringan, yang bisa menjadi tanda adanya upaya serangan. Banyak firewall modern memiliki kemampuan untuk memberikan laporan dan log aktivitas secara real-time, yang bisa sangat membantu dalam deteksi dini serangan dan penyelesaian masalah jaringan.

Selanjutnya, pemeliharaan firewall melibatkan peningkatan dan pembaruan secara reguler. Peningkatan mungkin diperlukan untuk menambah fungsionalitas atau meningkatkan kinerja, sedangkan pembaruan biasanya mencakup perbaikan bug dan pembaruan keamanan untuk melawan ancaman baru. Selain itu, aturan firewall mungkin perlu disesuaikan atau diperbarui berdasarkan perubahan dalam lalu lintas jaringan atau ancaman keamanan yang dihadapi.

10.4.1 Pembaruan dan peningkatan Firewall

Pembaruan dan peningkatan adalah bagian penting dalam siklus hidup manajemen dan pemeliharaan firewall. Kedua proses ini sangat vital untuk memastikan bahwa firewall terus bekerja dengan optimal dan tetap dapat melindungi jaringan dari ancaman yang selalu berkembang.

Pembaruan firewall umumnya melibatkan instalasi patch keamanan atau perbaikan bug yang telah ditemukan oleh produsen. Pembaruan ini sangat penting untuk melindungi jaringan dari ancaman terkini. Misalnya, jika ada celah keamanan yang ditemukan dalam perangkat lunak firewall, produsen biasanya akan merilis pembaruan untuk memperbaiki celah tersebut. Tanpa pembaruan ini, jaringan Anda mungkin rentan terhadap serangan.

Peningkatan firewall, di sisi lain, bisa melibatkan penambahan fungsionalitas atau peningkatan kinerja. Peningkatan bisa dalam bentuk penambahan modul keamanan baru, seperti

sistem pendeteksi intrusi, atau peningkatan kemampuan untuk mengelola lalu lintas jaringan yang besar. Peningkatan ini bisa menjadi penting ketika organisasi tumbuh dan kebutuhan jaringan berubah.

Sebelum melakukan pembaruan atau peningkatan, penting untuk melakukan pengetesan di lingkungan yang terkontrol. Ini membantu memastikan bahwa pembaruan atau peningkatan tidak akan mengganggu operasi normal atau menciptakan masalah baru. Selain itu, penting juga untuk memiliki rencana pemulihan jika ada sesuatu yang salah selama proses ini.

Sebagai bagian dari strategi pembaruan dan peningkatan, organisasi harus memiliki prosedur reguler untuk mengecek dan menerapkan pembaruan dari produsen. Proses ini harus dilakukan oleh profesional TI yang berpengalaman dan dengan pendekatan yang hati-hati untuk meminimalkan risiko.

Secara keseluruhan, pembaruan dan peningkatan adalah proses penting yang membantu menjaga firewall tetap efektif dalam melindungi jaringan Anda dari ancaman keamanan yang selalu berubah.

10.4.2 Pengawasan dan laporan Firewall

Pengawasan atau pemantauan firewall adalah proses berkelanjutan yang melibatkan melacak dan menganalisis lalu lintas jaringan yang melewati firewall secara real-time. Pengawasan ini penting untuk memastikan bahwa firewall berfungsi dengan baik dan melindungi jaringan Anda dari ancaman eksternal maupun internal.

Proses pengawasan mencakup identifikasi dan pemeriksaan paket data yang melewati firewall, penilaian peraturan firewall dan sejauh mana mereka diterapkan, serta deteksi aktivitas yang tidak biasa atau mencurigakan. Kegiatan ini membantu dalam mendeteksi serangan yang sedang berlangsung,

penyalahgunaan sistem, dan bahkan bisa menjadi langkah pertama dalam penyelidikan insiden keamanan.

Sementara itu, laporan firewall adalah ringkasan atau rekapitulasi terperinci dari data yang dikumpulkan selama proses pengawasan. Laporan ini umumnya mencakup statistik lalu lintas jaringan, detail tentang ancaman yang dideteksi, aktivitas yang dianggap mencurigakan, dan informasi tentang bagaimana firewall merespons berbagai jenis lalu lintas.

Firewall canggih saat ini biasanya dilengkapi dengan kemampuan untuk membuat laporan yang mendalam dan mudah dipahami. Laporan ini dapat memberikan gambaran yang jelas tentang aktivitas jaringan, performa firewall, dan ancaman potensial terhadap keamanan. Beberapa firewall bahkan menawarkan fungsionalitas untuk laporan real-time, yang memungkinkan Anda untuk melihat aktivitas jaringan saat ini dan merespons ancaman dalam waktu nyata.

Selain itu, laporan juga merupakan komponen penting dalam proses audit keamanan dan mematuhi regulasi industri. Mereka dapat digunakan untuk menunjukkan kepada auditor atau pengawas bahwa organisasi Anda mengambil langkah-langkah yang tepat untuk melindungi data dan informasi penting.

10.5 Keamanan dan Firewall: Tantangan dan Solusi

10.5.1 Ancaman keamanan yang dapat dicegah dengan Firewall

Firewall merupakan garda pertama yang melindungi jaringan dari berbagai ancaman keamanan yang ada di dunia maya. Mereka berfungsi sebagai benteng pertahanan dalam menangani serangan yang ditujukan untuk merusak, meretas, atau mencuri data dari sistem kita. Berikut adalah beberapa ancaman keamanan utama yang dapat dicegah dengan menggunakan firewall.

Serangan *Denial-of-Service* (DoS) dan *Distributed Denial-of-Service* (DDoS) adalah dua jenis serangan yang paling umum dihadapi oleh jaringan. Serangan ini dilakukan dengan cara membanjiri jaringan atau server dengan lalu lintas data yang sangat banyak, dengan tujuan untuk membuat jaringan atau server tersebut menjadi tidak dapat diakses. Firewall dapat membantu mencegah serangan jenis ini dengan membatasi jumlah lalu lintas yang dapat masuk ke jaringan.

Selanjutnya, serangan brute-force adalah upaya berulang-ulang untuk mendapatkan akses ke sistem dengan menebak kombinasi nama pengguna dan kata sandi. Firewall dapat membantu melawan serangan ini dengan memblokir alamat IP yang mencoba melakukan login secara berulang kali dalam waktu singkat.

Selain itu, serangan *man-in-the-middle* (MitM) adalah serangan di mana penyerang menyadap komunikasi antara dua pihak dan berpotensi memodifikasi atau mencuri data yang ditransmisikan. Firewall dapat mencegah serangan ini dengan mengenkripsi data yang dikirim dan diterima, serta dengan memverifikasi sumber data.

Phishing dan serangan malware lainnya juga dapat dicegah oleh firewall. Phishing biasanya dilakukan dengan mengirim email palsu yang tampak sah untuk mengelabui pengguna agar memasukkan informasi pribadi atau login. Sementara itu, malware adalah perangkat lunak jahat yang dapat merusak sistem atau mencuri data. Firewall dapat membantu melindungi terhadap serangan ini dengan memblokir akses ke situs web atau email yang mencurigakan dan dengan memindai file yang didownload untuk mencari tanda-tanda malware.

Secara keseluruhan, firewall merupakan alat keamanan penting yang dapat melindungi jaringan dari berbagai ancaman. Dengan pemahaman yang baik tentang ancaman yang ada dan

bagaimana firewall dapat membantu mencegahnya, kita dapat membuat jaringan yang lebih aman dan tangguh.

10.5.2 Keterbatasan dan kelemahan Firewall

Meski *firewall* memiliki banyak kegunaan dalam melindungi jaringan dan sistem kita dari ancaman keamanan, namun tetap ada keterbatasan dan kelemahan yang perlu kita ketahui dan tangani dengan baik. Berikut adalah beberapa keterbatasan dan kelemahan dari firewall:

1. *False Positives* dan *False Négatives*. Salah satu tantangan utama dalam penggunaan *firewal*l adalah menciptakan keseimbangan antara keamanan dan kenyamanan pengguna. Jika aturan *firewall* terlalu ketat, dapat menghasilkan "*false positives*" dimana lalu lintas jaringan yang sah dianggap sebagai ancaman dan diblokir. Sebaliknya, jika aturan *firewall* terlalu longgar, dapat terjadi "*false negatives*" dimana lalu lintas jaringan yang berbahaya dianggap sah dan diizinkan masuk.
2. Tidak bisa melindungi dari ancaman internal. Firewall umumnya efektif melindungi jaringan dari ancaman eksternal, tetapi tidak sepenuhnya efektif melawan ancaman internal. Misalnya, jika seorang karyawan secara tidak sengaja mengunduh malware, atau jika seseorang dengan akses jaringan melakukan aktivitas yang merusak, firewall mungkin tidak mampu mencegah ini.
3. Kurangnya perlindungan terhadap social engineering. Firewall dapat memblokir lalu lintas jaringan yang mencurigakan, tetapi tidak bisa melindungi pengguna dari teknik social engineering. Misalnya, jika seorang pengguna dibujuk untuk mengungkapkan password atau informasi pribadi lainnya, firewall tidak bisa mencegahnya.
4. Diperlukan pemeliharaan dan pembaruan. Untuk menjaga efektivitasnya, firewall perlu dirawat dan diperbarui secara

berkala. Jika firewall tidak diperbarui dengan tepat, hal ini dapat menimbulkan celah keamanan yang bisa dimanfaatkan oleh penyerang.

5. Hanya bagian dari solusi keamanan. Meski firewall penting, namun tidak bisa dijadikan solusi keamanan tunggal. Firewall harus digunakan sebagai bagian dari strategi keamanan yang lebih luas yang mencakup perangkat lunak anti-virus, kontrol akses, pelatihan keamanan bagi pengguna, dan langkah-langkah lainnya.

Memahami keterbatasan dan kelemahan ini dapat membantu kita merencanakan dan menerapkan strategi keamanan yang lebih holistik dan efektif.

10.5.3 Teknologi dan pendekatan baru dalam Firewall

Seiring berjalannya waktu, berbagai teknologi dan pendekatan baru telah diimplementasikan untuk meningkatkan efektivitas dan efisiensi firewall. Bukan hanya dalam hal deteksi dan pencegahan ancaman, tetapi juga dalam hal manajemen dan pemeliharaan.

1. *Firewall* Berbasis *Cloud*. Seiring dengan semakin banyaknya organisasi yang beralih ke solusi berbasis cloud, konsep firewall berbasis cloud atau cloud-based firewall juga semakin populer. Firewall berbasis cloud ini memiliki keuntungan dalam hal fleksibilitas, scalability, dan pemeliharaan. Dengan *firewall* berbasis *cloud*, organisasi dapat dengan mudah menyesuaikan kapasitas mereka sesuai dengan kebutuhan dan mendapatkan pembaruan dan pemeliharaan dari penyedia layanan cloud.
2. *Firewall* sebagai Layanan (FWaaS). Konsep ini menggabungkan firewall dengan model layanan berbasis *cloud*. Dengan FWaaS, organisasi dapat mengakses dan mengelola firewall mereka melalui platform berbasis cloud.

Ini memungkinkan organisasi untuk mengendalikan kebijakan keamanan mereka secara sentralisasi dan konsisten di seluruh jaringan mereka, termasuk untuk lokasi yang berbeda dan lingkungan multi-cloud.

3. Integrasi dengan Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS). Sebagai tambahan terhadap fungsi firewall tradisional, beberapa solusi firewall kini juga mencakup fitur deteksi dan pencegahan intrusi. Dengan mengintegrasikan IDS/IPS, firewall dapat lebih efektif dalam mendeteksi dan merespons ancaman yang lebih canggih dan rumit.
4. Otomatisasi dan Orkestrasi. Mengelola dan mengatur firewall dapat menjadi tugas yang rumit dan memakan waktu, terutama untuk jaringan yang besar dan kompleks. Oleh karena itu, banyak solusi firewall kini menawarkan fitur otomatisasi dan orkestrasi. Misalnya, otomatisasi aturan dan kebijakan firewall, otomatisasi respon terhadap ancaman, dan orkestrasi dengan sistem keamanan lainnya.

Pengembangan dan penyebaran teknologi dan pendekatan baru dalam firewall adalah hal yang penting dalam melindungi jaringan dan sistem kita dari ancaman keamanan yang terus berkembang. Namun, penting untuk selalu mempertimbangkan kebutuhan dan konteks spesifik organisasi kita dalam memilih dan menerapkan solusi firewall.

Saat ini, salah satu pendekatan yang sedang tumbuh dan berkembang adalah penggunaan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dalam pengaturan dan operasional firewall.

AI dan ML dapat memberikan keuntungan signifikan dalam penggunaan firewall. Misalnya, AI dan ML dapat digunakan untuk otomatisasi dan peningkatan efisiensi dalam pengaturan dan pengoperasian firewall. Penggunaan AI dapat membantu meminimalkan kesalahan manusia dalam penyetelan dan

pemeliharaan firewall. Selain itu, dengan kemampuan ML untuk belajar dari data dan mengidentifikasi pola, dapat memperkuat deteksi ancaman dan merespons lebih cepat terhadap serangan.

AI dan ML juga dapat digunakan dalam pendekatan berbasis perilaku atau *'behavioral-based'* dalam firewall. Alih-alih hanya bergantung pada aturan yang telah ditetapkan sebelumnya, pendekatan ini menggunakan ML untuk belajar dari lalu lintas jaringan yang terus berubah dan mengadaptasi diri untuk mendeteksi aktivitas yang tidak biasa atau mencurigakan. Ini berarti bahwa firewall dapat menjadi lebih responsif dan akurat dalam mendeteksi ancaman baru dan kompleks.

Selain itu, penggunaan AI dan ML dalam firewall juga bisa membantu dalam memahami dan menangani *'zero-day attacks'*, yaitu serangan yang memanfaatkan kerentanan yang belum dikenal atau belum ada perbaikannya. ML dapat digunakan untuk mengidentifikasi pola dan anomali yang mungkin menunjukkan serangan jenis ini, sehingga memungkinkan respons yang lebih cepat dan efektif.

Meski begitu, penting untuk diingat bahwa penggunaan AI dan ML dalam firewall juga datang dengan tantangan sendiri. Misalnya, diperlukan data besar dan relevan untuk melatih model ML, dan juga perlu dilakukan penyesuaian dan pemeliharaan secara berkala untuk menjaga efektivitasnya. Selain itu, seperti teknologi lainnya, AI dan ML juga dapat menjadi target serangan oleh penyerang yang canggih dan berpengetahuan.

10.6 Kasus Studi: Firewall dalam Praktek

10.6.1 Penggunaan Firewall dalam bisnis

PT. XYZ merupakan sebuah perusahaan rintisan (*startup*) di bidang teknologi finansial (*fintech*) yang berbasis di Jakarta. Perusahaan ini menawarkan layanan digital dalam bentuk aplikasi untuk melakukan transaksi keuangan seperti transfer uang, pembayaran tagihan, dan lain sebagainya. Mengingat perusahaan

bergerak di bidang fintech, informasi dan data yang diolah dan disimpan sangat sensitif, seperti data keuangan dan data pribadi pengguna.

Seiring pertumbuhan perusahaan dan jumlah pengguna yang meningkat, PT. XYZ mulai menghadapi tantangan dalam menjaga keamanan data dan sistem mereka. Perusahaan ini sering kali menjadi target serangan cyber, mulai dari percobaan akses ilegal, serangan DDoS, hingga serangan malware dan ransomware.

Untuk mengatasi tantangan ini, PT. XYZ memutuskan untuk menerapkan firewall dalam sistem keamanan mereka. Perusahaan ini menggunakan model firewall berbasis cloud (*cloud-based firewall*) yang dapat disesuaikan dengan skala dan kebutuhan mereka. Firewall ini diatur untuk memblokir lalu lintas yang mencurigakan dan melindungi sistem dari akses ilegal.

Selain itu, PT. XYZ juga menggunakan fitur IDS/IPS yang terintegrasi dengan firewall untuk mendeteksi dan merespons serangan yang lebih canggih. Misalnya, untuk mendeteksi dan mencegah serangan DDoS yang bertujuan untuk mengganggu layanan mereka.

Dalam praktiknya, penggunaan firewall di PT. XYZ telah membantu perusahaan ini dalam menjaga keamanan sistem dan data mereka. Selain itu, penggunaan firewall juga membantu membangun kepercayaan pengguna, karena mereka merasa lebih aman dalam menggunakan layanan perusahaan ini.

Dalam implementasi firewall, PT. XYZ menerapkan serangkaian aturan yang didesain untuk menangani berbagai jenis ancaman. Beberapa contoh aturan yang diterapkan adalah:

1. Pemblokiran Lalu Lintas dari IP Tertentu. Firewall diatur untuk memblokir lalu lintas dari alamat IP yang telah diketahui mencoba melakukan serangan atau aktivitas mencurigakan ke sistem perusahaan.
2. Pembatasan Akses ke Port Tertentu. PT. XYZ juga menerapkan aturan untuk membatasi akses ke port

tertentu dalam rangka mencegah akses tidak sah. Misalnya, port yang digunakan untuk layanan internal perusahaan dibatasi hanya bisa diakses oleh alamat IP tertentu.

3. Pemblokiran Protokol Tertentu. PT. XYZ menggunakan firewall untuk memblokir protokol yang tidak dibutuhkan atau berisiko tinggi. Misalnya, firewall diatur untuk memblokir semua lalu lintas ICMP untuk mencegah serangan DDoS.
4. Pembatasan Akses ke Situs Web Tertentu. Selain itu, perusahaan juga menggunakan firewall untuk memblokir akses ke situs web tertentu yang dapat digunakan untuk melakukan serangan phishing atau menyebarkan malware.
5. Penerapan Kebijakan "*Default Deny*". Sebagai pendekatan yang lebih proaktif, PT. XYZ menerapkan kebijakan "default deny", di mana semua lalu lintas jaringan diblokir secara default kecuali yang telah ditentukan sebelumnya dalam aturan firewall.

Aturan-aturan ini dirancang dan disesuaikan berdasarkan kebutuhan dan konteks keamanan PT. XYZ. Seiring berjalannya waktu, perusahaan ini melakukan evaluasi dan pembaruan secara berkala terhadap aturan firewall mereka untuk memastikan bahwa mereka tetap efektif dalam melindungi sistem dan data perusahaan.

Berikut adalah aturan firewall menggunakan format IPTables.

Tabel 10.2. Tabel Aturan Firewall pada PT. XYZ dengan format IPTables

Aturan	Perintah
Blokir IP Tertentu	iptables -A INPUT -s 192.168.1.100 -j DROP
Batasi Akses Port	iptables -A INPUT -p tcp --destination-port 22 -s 192.168.1.1 -j ACCEPT iptables -A INPUT -p tcp --destination-port 22 -j DROP
Blokir Protokol	iptables -A INPUT -p icmp -j DROP
Batasi Akses Situs Web	iptables -A FORWARD -m string --string "www.facebook.com" -j DROP
Kebijakan "Default Deny"	iptables -P INPUT DROP iptables -P FORWARD DROP iptables -P OUTPUT DROP

10.6.2 Penggunaan Firewall dalam pemerintahan

Untuk ilustrasi penggunaan firewall dalam pemerintahan, kita dapat melihat studi kasus Departemen Pertahanan Republik Indonesia. Departemen ini merupakan bagian penting dalam pemerintahan yang harus melindungi informasi dan data yang sangat penting dan rahasia. Untuk itu, penggunaan firewall sangat diperlukan.

Sebagai sebuah departemen yang bergerak dalam bidang pertahanan, tentu ada banyak ancaman siber yang harus dihadapi. Mulai dari serangan DoS (*Denial of Service*), DDoS (*Distributed Denial of Service),* hingga ancaman malware dan spyware. Menghadapi hal tersebut, firewall digunakan sebagai benteng pertama yang melindungi jaringan departemen dari serangan-serangan ini.

Departemen Pertahanan menggunakan *firewall* jenis *Stateful Inspection Firewall*. Ini karena jenis *firewall* ini mampu memfilter paket data berdasarkan konteks dan keadaan sesi koneksi, sehingga lebih efektif dalam mencegah ancaman siber yang lebih canggih. Selain itu, untuk melindungi dari serangan DoS dan DDoS, departemen juga menggunakan teknologi pembatasan rate dan filtrasi IP spoofing.

Aturan firewall yang diterapkan oleh departemen pertahanan mencakup blokir lalu lintas dari IP yang mencurigakan, pembatasan akses ke port tertentu, blokir protokol yang berisiko, dan penerapan kebijakan "*default deny*".

Misalnya, perintah IPTables untuk memblokir lalu lintas dari IP yang mencurigakan bisa seperti ini:

iptables -A INPUT -s [IP mencurigakan] -j DROP

Sementara itu, untuk membatasi akses ke port tertentu, perintahnya mungkin seperti ini:

iptables -A INPUT -p tcp --destination-port 22 -j DROP

Departemen juga membatasi protokol yang berisiko dengan perintah:

iptables -A INPUT -p icmp -j DROP

Dan menerapkan kebijakan "default deny" dengan perintah:

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT DROP

Dalam melakukan semua pengaturan ini, departemen bekerja sama dengan tim IT profesional dan melakukan peninjauan rutin untuk memastikan bahwa aturan dan sistem keamanan jaringan tetap efektif dan *up-to-date*.

10.6.3 Penggunaan Firewall dalam sektor pendidikan

Penggunaan firewall dalam sektor pendidikan juga sangat penting. Dalam konteks ini, kita akan membahas tentang sebuah universitas ternama di Indonesia. Dengan ribuan mahasiswa dan staf pengajar yang terkoneksi dalam satu jaringan, universitas ini perlu menjaga agar data dan informasi yang ada di jaringan tersebut terlindungi.

Universitas ini menggunakan firewall jenis Application Layer Firewall. Jenis firewall ini memungkinkan kontrol lalu lintas data yang lebih detil berdasarkan aplikasi atau layanan yang digunakan. Misalnya, universitas dapat mengizinkan lalu lintas data dari aplikasi email dan aplikasi e-learning, namun memblokir lalu lintas data dari aplikasi permainan online yang dapat mengganggu konsentrasi belajar mahasiswa.

Firewall juga digunakan untuk membatasi akses ke situs-situs tertentu yang tidak relevan dengan kegiatan belajar mengajar. Misalnya, situs perjudian dan situs konten dewasa diblokir agar tidak dapat diakses dari jaringan universitas.

10.7 Penutup

Sebagai penutup dari buku ini, kita dapat merangkum bahwa *firewall* merupakan komponen keamanan jaringan yang sangat penting. Dari mulai definisi, fungsi, jenis-jenis, hingga cara kerjanya, semua telah kita bahas dalam buku ini. Studi kasus yang telah kita ulas juga membuktikan betapa pentingnya peran firewall dalam berbagai sektor, mulai dari bisnis, pemerintahan, hingga pendidikan.

Namun, perlu diingat bahwa meski firewall merupakan lapisan pertama dalam sistem keamanan jaringan, itu tidak berarti kita dapat mengandalkan firewall saja dalam melindungi jaringan dari ancaman siber. Selalu ada keterbatasan dan kelemahan dalam setiap sistem, termasuk *firewall*. Oleh karena itu, penting bagi kita untuk terus mengupdate dan meningkatkan sistem keamanan

jaringan kita, serta menggunakan lapisan-lapisan keamanan lainnya seperti IDS/IPS, antivirus, dan lainnya. Selain itu, kemajuan teknologi juga berarti bahwa ancaman siber juga terus berkembang dan menjadi semakin canggih. Oleh karena itu, kita juga perlu terus mempelajari dan menerapkan teknologi dan pendekatan baru dalam sistem firewall kita, seperti penerapan *Artificial Intelligence* dan *Machine Learning*.

Akhir kata, kami berharap buku ini dapat memberikan pemahaman yang baik kepada pembaca tentang firewall, serta menjadi panduan yang bermanfaat dalam melindungi jaringan Anda dari ancaman siber. Ingatlah bahwa dalam dunia siber, keamanan adalah hal yang paling penting. Selalu berhati-hati dan tetap aman!

DAFTAR PUSTAKA

Chapman, D.B. 1992. 'Network (In)Security Through IP Packet Filtering', in. USENIX Summer.

Cheswick, W. *et al.* 2003. *Firewalls and Internet Security: Repelling the Wily Hacker*. 2nd edn. Addison-Wesley Professional.

Cisco. 2021. *What Is a Firewall?* Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.

Eddy, W. 2007. 'TCP SYN Flooding Attacks and Common Mitigations', *Verizon* [Preprint].

Ferguson, P. and Huston, G. 1998. *Quality of service: delivering QoS on the Internet and in corporate networks*. New York, NYUnited States: John Wiley & Sons, Inc.

Mirkovic, J. and Reiher, P. 2004. 'A taxonomy of DDoS attack and DDoS defense mechanisms', *ACM SIGCOMM Computer Communication Review*, 34(2), pp. 39–53. Available at: https://doi.org/10.1145/997150.997156.

Stallings, W. and Brown, L. 2018. *Computer Security: Principles and Practice*. 4th editio. Pearson.

Zeltser, L. *et al.* 2002. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Vpns, Routers, and Intrusion Detection Systems*. Sams.

Zwicky, E.D., Cooper, S. and Chapman, D.B. 2000. *Building Internet Firewalls*. O'Reilly Media, Inc.

BAB 11
INTRUSION DETECTION SYSTEM

Oleh Shah Khadafi

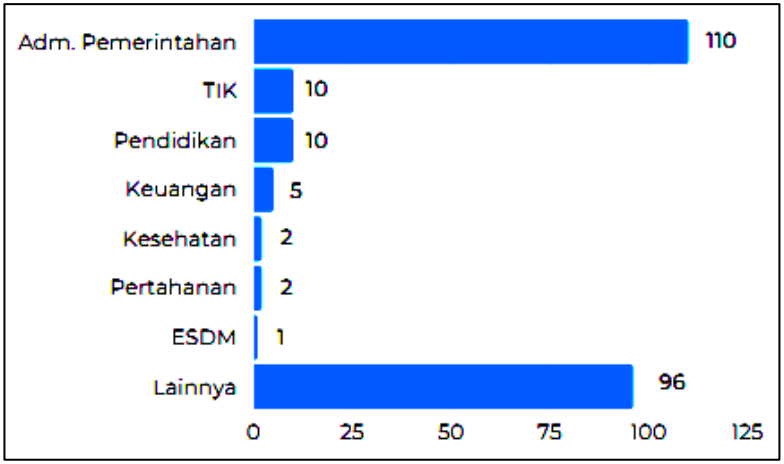
11.1 Pendahuluan

Saat ini dunia komputasi bisnis dihadapkan pada kemungkinan trafik anomaly yang tidak diketahui yang terus meningkat karena berbagai serangan dan pelanggaran keamanan. Dalam lingkungan ketidakamanan yang selalu dihantui dengan ancaman dari peretas dan ancaman berbahaya dari virus, perusahaan-perusahaan di seluruh dunia berusaha menjaga kesinambungan layanannya (yaitu bertahan dalam sistem) dan mempertahankan daya komputasi, menikmati keunggulan kompetitif yang signifikan. Sesuai dengan laporan Badan Siber dan Sandi Nasional (BSSN) - Direktorat Operasi Keamanan Siber, trafik anomaly yang terjadi di Indonesia pada tahun 2022 sebanyak 976,429,996 (Direktorat Operasi Keamanan Siber, 2022).

Dampak trafik anomaly mengakibatkan kerugian finansial dan lebih banyak kerugian bagi kredibilitas perusahaan komersial terutama dari pihak pemerintah, maupun dari pihak yang lain. Tercatat aduan kejahatan cyber yang diterima oleh BSSN yang tertinggi dari sektor pemerintahan sebanyak 100 kasus, dari perusahaan TIK 10, bidang pendidikan 10, lembaga keuangan 5, insitutsi kesehatan 2, bidang pertahanan 2, bidang ESDM 1 aduan, dan yang terakhir bidang-bidang lainnya sebanyak 96 aduan. Statistik aduan permasalahan *cyber security* disajikan pada gambar 11.1.

Terkait dengan berbagai macam aktivitasi *anomaly* yang terjadi di Indonesia, dimana target serangannya mengancam berbagai sektor industri baik pemerintah maupun swasta. Aktivitas

seraangan *anomaly* bisa terjadi dikarenakan otomasi perangkat keras atau perangkat lunak apa pun yang digunakan yang mendukung kinerja dalam melakukan akses terhadap *resource* sebuah sistem komputer. Sehingga, diperlukan kegiatan yang memantau, mendeteksi, atau merespons peristiwa anomaly yang terjadi melalui trafik jaringan dan masuk di komputer host yang dianggap relevan dengan pendekatan detection intrusion.

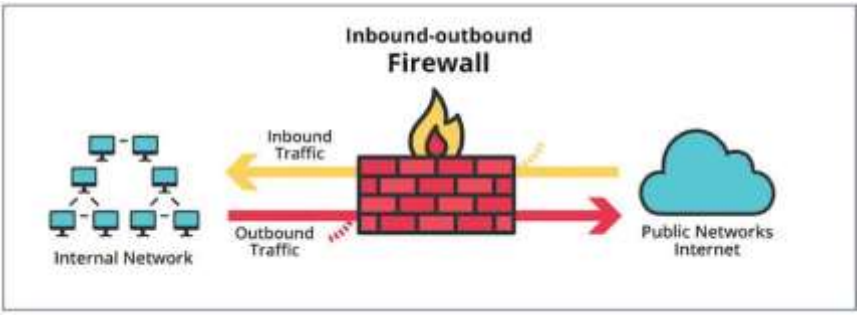


Gambar 11.1. Statistik Aduan Serangan Cyber di Indonesia (Sumber : https://bssn.go.id/monitoring-keamanan-siber-2022/)

11.2 Perbedaan IDS dan Firewall

Perbedaan antara *firewall* dengan IDS dapat dilihat dari aktivitas monitoring jaringan. *Firewall* memantau semua *inbound and outbound traffic* dan mendeteksi kemungkinan upaya intrusi berdasarkan informasi tertentu alamat IP, nomor port, protokol tertentu yang digunakan, dll. Firewall dapat memberlakukan *rules* terhadap sebuah lalu lintas jaringan seperti memblokir, mengizinkan, dan menolak lalu lintas yang mengandung informasi paket data tertentu (Khadafi *et al.,* 2019). Sedangkan, IDS mendeteksi penyusup dengan cara memeriksa lalu lintas yang

terpantau yang kemudian membandingkannya dengan *signature of malicious threats* (yang telah tersimpan sebelumnya), Perbandingan ke dua aktivitas trafik jaringan yang masuk dalam sistem, kemudian dapat diketahui dasar pola atau perilakunya, yang kemudian menghasilkan *alert* kepada administrator sistem jika trafik yang terpantau mengandung upaya *malicious threats*.



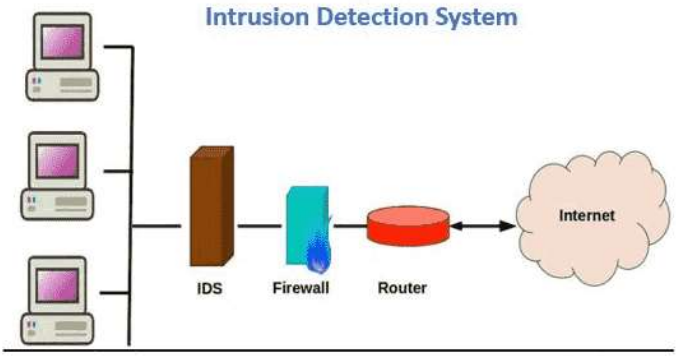
Gambar 11.2. Cara Kerja Firewall
(Sumber : https://www.comodo.com/ids-in-security.php)

11.3 Intrusion Detection System (IDS)

Konsep *detection intrusion* pertama kali diperkenalkan oleh James P. Anderson dalam paper penelitian yang berjudul "*Computer security threat monitoring and surveillance*" pada tahun 1980. Penelitian yang dilakukan oleh James, yaitu merancang sistem pengawasan pemantauan keamanan terhadap jenis-jenis *threats* dan *attack* yang dapat dipasang di dalam sistem komputer, dan bagaimana ancaman dapat terekam dalam analisis data audit (Anderson, 1980). Dengan cara menganalisis *log file* yang memberikan informasi penting untuk menentukan apakah ada penggunaan yang tidak normal.

Intrusion Detection adalah proses mengidentifikasi dan merespons aktivitas jahat yang ditargetkan pada komputasi dan sumber daya jaringan, yang juga dapat melakukan pencegahan apabila pada sebuah aliran trafik jaringan berupa paket datanya

mengandung *threats,* seperti yang diilustrasikan pada gambar 11.3. Dimana, penyerang mampu mengeksploitasi *vulnerability* kelemahan yang terdapat pada sistem komputer target (bisa jadi sebuah komputer *server*) dengan cepat ketika berhasil memasuki sistem jaringan (Khadafi *et al.,* 2017). IDS dapat melakukan pemeriksaan dan identifikasi paket data dari trafik jaringan tanpa harus melakukan *signature* terlebih dahulu dari *threats* yang dimaksud. IDS berupa sebuah sistem aplikasi yang dapat memonitor lalu lintas jaringan dari aktivitas paket-paket data yang mencurigakan atau yang melanggar aturan keamanan jaringan dan kemudian membuat laporan dari aktivitas jaringan tersebut.



Gambar 11.3. Cara Kerja IDS
(Sumber : https://www.comodo.com/ids-in-security.php)

IDS salah satu komponen terpenting dari arsitektur keamanan jaringan modern adalah IDS, yang memungkinkan identifikasi awal serangan untuk dapat mendeteksi dan memberikan kesempatan untuk menguranginya, yang kemudian membunyikan alarm ketika mendeteksi aktivitas jahat. Selain itu, IDS memungkinkan deteksi berbagai serangan, misalnya: *Denial of Service* (DoS), *Man in the Middle* (MitM), dll. IDS dapat memantau dan mencatat setiap, dan semua, lalu lintas jaringan seperti yang

ditentukan. Karena IDS dapat memberikan perincian tentang serangan saat terjadi, ini membantu administrator keamanan untuk memahami apa yang telah terjadi. Oleh karena itu, jika terjadi serangan serupa di masa mendatang, keamanan sistem dapat dikonfigurasi untuk mendeteksi dan mencegah serangan yang termasuk dalam kategori IDS.

11.4 Kategori Serangan IDS

Ada tiga kategori serangan *detection intrusion* yang termasuk dalam serangan IDS: *misuse detection*, *anomaly detection*, dan hybrid detection (Varal & Wagh, 2018).

11.4.1 Misuse detection

Misuse detection juga dikenal sebagai *signature detection* (deteksi tanda tangan), mencari pola intrusi yang diketahui di jaringan atau di host. Setiap serangan memiliki tanda khusus, misalnya, dapat berupa muatan paket, alamat IP sumber, atau header tertentu. IDS dapat membunyikan alarm jika mendeteksi serangan yang memiliki salah satu tanda tangan yang tercantum dalam daftar tanda tangan yang diketahui dari IDS. Keuntungan dari pendekatan ini adalah akurasinya yang tinggi untuk mendeteksi serangan yang diketahui. Namun, kelemahannya adalah tidak efisien terhadap pola serangan yang belum terdeteksi sebelumnya atau *zero-day attack*.

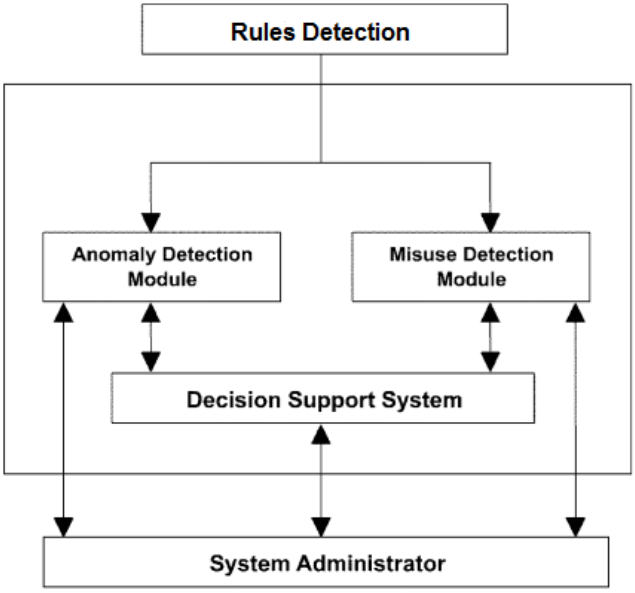
11.4.2 Anomaly Detection

Anomaly detection mendefinisikan keadaan normal jaringan atau host, yang disebut garis dasar, dan setiap penyimpangan dari garis dasar ini dilaporkan sebagai serangan potensial. Misalnya, IDS berbasis anomali dapat membuat garis dasar berdasarkan lalu lintas jaringan umum seperti layanan yang disediakan oleh setiap host, layanan yang digunakan oleh setiap host, dan volume aktivitas sepanjang hari. Jadi, jika penyerang mengakses sumber daya internal pada tengah malam, dan jika di baseline hampir tidak

ada aktivitas pada tengah malam, maka IDS akan membunyikan alarm. Keuntungan dari deteksi anomali adalah fleksibilitasnya untuk menemukan serangan intrusi yang tidak diketahui. Namun, dalam kebanyakan kasus, sulit untuk secara tepat menentukan garis dasar jaringan, sehingga tingkat deteksi palsu dari teknik ini bisa tinggi (Mansyur, 2020).

11.4.3 Hybrid Detection

Untuk mengatasi kelemahan dari dua metode deteksi intrusi konvensional, *misuse detection* dan *anomaly detection*, hybrid detection ini menggabungkan kedua-duanya. Arsitektur IDS terdiri dari modul *anomaly detection*, modul *misuse detection*, dan *decision support system* (sistem pendukung keputusan) yang menggabungkan hasil dari dua modul deteksi.



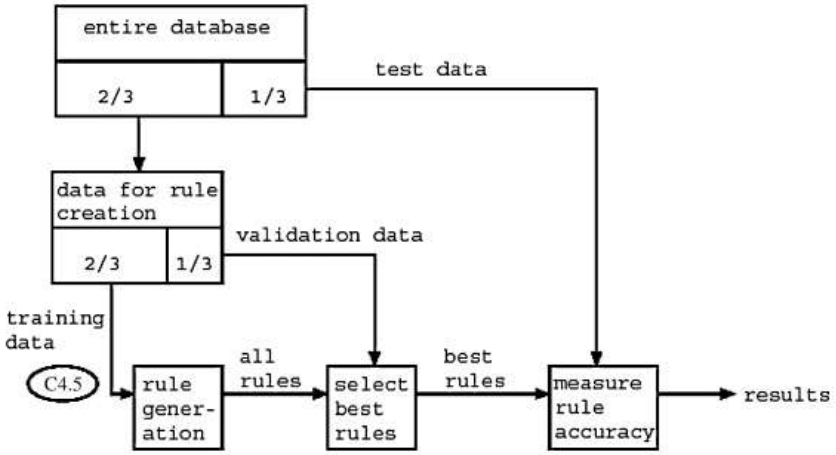
Gambar 11.4. Arsitektur *Hybrid Detection*
(Sumber : Varal & Wagh, 2018)

Arsitektur *Hybrid detection* diilustrasikan seperti yang nampak pada gambar 11.4. Pada gambar tersebut terdapat blok bagian antara lain yaitu:

1. *Anomaly detection* adalah faktor terpenting dari *intrusion detection* yang dapat mengenali dan mengidentifikasi penyimpangan atau kejanggalan aktivitas trafik yang terjadi pada lalu lintas jaringan normal, sehingga dapat mengetahui adanya serangan atau kesalahan yang disengaja atau tidak disengaja. Deteksi ini dilakukan dengan cara mencatat setiap koneksi yang sedang dipantau dan memeriksa fitur lalu lintas dasar yang diekstrak. Di dalam *anomaly detection* terdapat tiga sub modul, yaitu (1) *preprocessing*, dimana di dalam *anomaly detection* terdapat algoritma yang dapat melakukan *training* terhadap *hybrid detection system* dengan data trafik normal dan memodelkan lalu lintas jaringan normal dari kumpulan data normal yang diberikan. Kemudian, dilakukan penentuan apakah data yang diuji tergolong dalam kategori 'normal' atau 'abnormal' dari data uji baru yang diberikan. (2) *anomaly analyzer modules*, dimana masing-masing analyzer melakukan analisa terhadap komunikasi penggunaan port TCP, UDP, dan ICMP. Pada modul ini menghasilakn sebuah profil keputusan apakah koneksi jaringan tergolong dalam kategori 'normal' atau 'abnormal'. (3) *communication modules*, untuk menangani komunikasi melalui Sistem Pendukung Keputusan (SPK).
2. *Misuse detection* adalah sebuah teknik *intrusion detection* yang di dalamnya mempunyai *rule-based* (berbasis aturan). *Rule-based* tersebut berisikan skenario serangan-serangan yang terjadi. Mekanisme *misuse detection* mengidentifikasi serangan yang berpotensi terjadi dari aktivitas user yang ditemukan, dimana aktivitas serangannya sesuai dengan *rules* yang telah ditetapkan di dalam *database*.

Pemberlakuan *rules* untuk *intrusion detection system* secara komprehensif menggunakan implementasi *expert system*.
Di dalam *misuse detection*, skenario dan karakteristik serangan baik dari data-datanya atau dari lalu lintas normal telah ditentukan sebelumnya. Karakteristik ini dikenal sebagai *signature of attack*, yang menjadi bagian dari *database of attack signatures*. Implementasi *misuse detection* pada *intrusion detection system* ini menggunakan algoritma decision tree yang dapat mengklasifikasikan serangan yang terjadi.

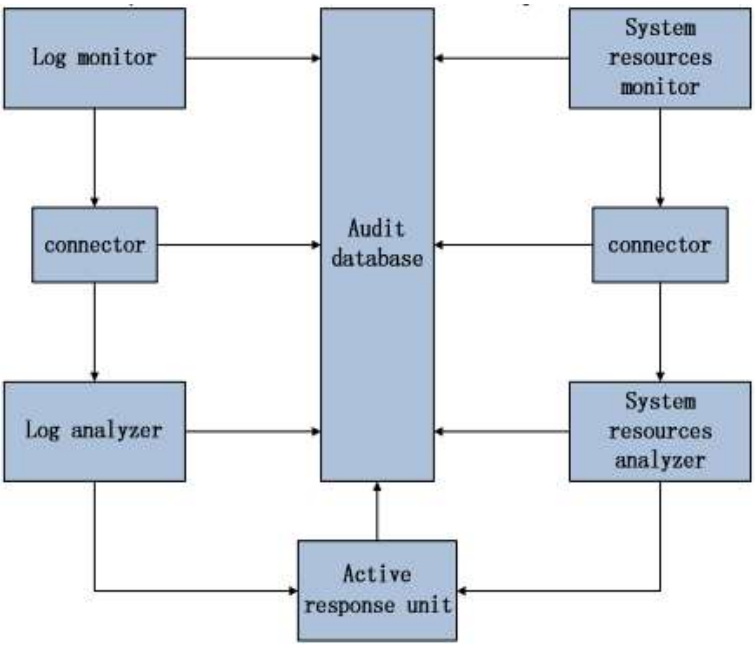
3. Decision support system, adalah modul terakhir dari arsitektur IDS yang diusulkan yang dapat melaporkan aktivitas *intrusion detection* kepada user, dan bertanggung jawab untuk menginterpretasikan hasil modul *anomaly detection* dan *misuse detection*.
4. *Rules*, di dalam blok rules berisikan aturan-aturan scenario deteksi serangan klasifikasi serangan yang terjadi.
    a. Jika modul *anomaly detection* dan *misuse detection* mendeteksi adanya serangan, maka deteksi tersebut adalah serangan dan *misuse detection* mengklasifikasikan serangan yang teridentifikasi.
    b. Jika modul *anomaly detection* tidak mendeteksi serangan dan *misuse detection* mendeteksi adanya serangan, maka deteksi tersebut adalah serangan dan *misuse detection* mengklasifikasikan serangan yang teridentifikasi.
    c. Jika modul *anomaly detection* mendeteksi serangan dan *misuse detection* tidak mendeteksi adanya serangan, maka deteksi tersebut adalah serangan yang tidak didefinisikan sebagai serangan yang tidak dapat diklasifikasikan.



Gambar 11.5. Strukur rules untuk IDS
(Sumber : Varal & Wagh, 2018)

11.5 *Host Intrusion Detection System* (HIDS)

HIDS melakukan pemantauan data dari trafik jaringan dari komputer host yang dipantaunya (Lin *et al.,* 2010). HIDS berbasis analisis *log* mencakup beberapa bagian berikut: pengumpulan data *file log*, *pre-decode log file*, *decoding file log*, analisis *log file*, dan laporan kejadian. File *log* melakukan perekaman aktivitas sebuah komputer *host* terhadap keseluruhan semua proses tindakan sistem operasi, aplikasi, dan perilaku penggunaan. File log banyak digunakan untuk *debugging sistem*, pemantauan, dan deteksi keamanan. Dengan demikian, sistem *log* sangat penting dalam *intrusion detection* dan alat analisis file *log* telah menjadi alat yang sangat diperlukan untuk inspeksi harian dan pemeliharaan sistem yang sedang berjalan. HIDS menggabungkan dua pendekatan *misuse detection* dan *anomaly detection* yang secara blok diagram nampak pada gambar di bawah ini.



Gambar 11.3. Blok Diagram IDS
(Sumber : Lin et al., 2010)

Pada gambar 11.3, keterangan masing-masing blok diagram IDS dijelaskan sebagai berikut, pertama kali blok *log monitor* memantau aktivitas-aktivitas sistem *application, security*, dan *system* yang terjadi. Aktivitas tersebut dilihat berdasarkan pada *file log* yang mencatat semua aktivitas *host system*. Ketika terjadi perubahan, pada *file log* akan segera mengirimkannya peristiwa ke blok *log analyzer*. Sedangkan, blok *system resource monitor* melakukan pemantauan terhadap *resource* sistem *host*, dan mengirimkan hasilnya berupa status penggunaan *resource* sistem ke blok s*ystem resource analyzer* yang menyesuaikan waktu dari sistem host. Blok *connector* menerima pesan dari *log monitor* dan *system resource monitor*, kemudian mengirimkannya ke blok *log analyzer* dan blok *system resource analyzer.* Blok *log analyzer*

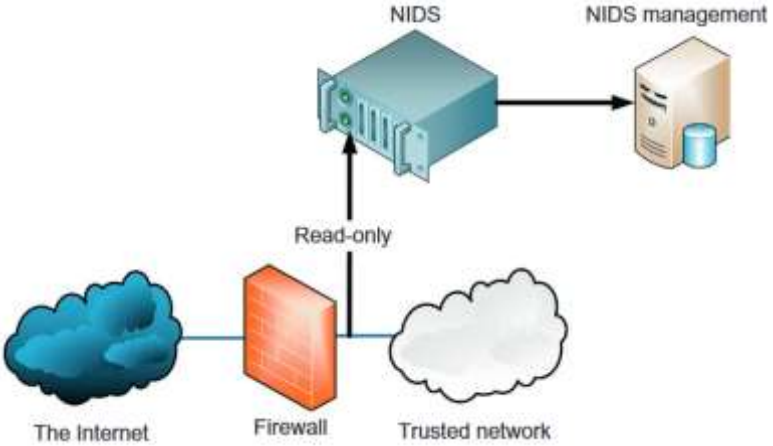
menganalisa kejadian dari *log monitor* yang kemudian membandingkannya dengan *rule-based* HIDS, jika terdapat kejadian yang mengandung invasi, maka melaporkannya ke blok *active response unit*. Kejadian serupa pada blok *system resource analyzer* yang menganalisa kejadian pada *resource* sistem yang sedang digunakan, jika ditemukan kejadian yang abnormal (anomaly) terhadap penggunaan *resource* host sistem, dan statusnya sedang diserang, jika ditemukan adanya invasion (serangan), maka melaporkannya ke *active response unit*. Blok *active response unit* menerima semua kejadian dari *log analyzer* dan *System resource analyzer*, dan kemudian memutuskan melakukan jenis apa operasi antisipasi yang dilakukan terhadap sistem *host*. Biasanya, operasi normal termasuk memberi tahu pengguna, audit, pemutusan dari jaringan dan sebagainya. Dan yang terakhir, blok *audit database* melakukan perekamana keseluruhan proses *intrusion detection*, dan juga situasi serangan, dan bersiap untuk digunakan bila diperlukan.

Implementasi HIDS dipasang di host dan memiliki akses ke detail seperti pengaturan registri, log, dan informasi sistem lainnya, mereka dapat membuat atribusi alamat IP dan forensik digital lebih mudah diakses. Namun, sumber daya diambil dari host (misalnya komputer tempat HIDS diinstal) untuk memberi daya pada HIDS dan HIDS bersifat reaktif dan hanya dapat merespons serangan setelah terjadi.

11.6 Network Intrusion Detection System

NIDS mendeteksi lalu lintas *malicious* di dalam jaringan, yang biasanya membutuhkan akses jaringan *promiscuous* untuk menganalisis semua lalu lintas, termasuk semua lalu lintas *unicast* (Conrad *et al.,* 2017). Jaringan dengan mode *promiscuous* yaitu dapat melakukan "*listening*" (mendengarkan) trafik sehingga dapat melakukan *capture* semua aliran data trafik jaringan, yang tidak hanya trafik yang masuk dalam workstation itu sendiri, tapi juga

dapat *capture* trafik untuk workstation yang lain (Ariyanto & Asmunin, 2018).



Gambar 11.4. Topologi NIDS
(Sumber : Conrad et al., 2017)

Peranti NIDS biasanya berupa perangkat keras pasif yang dipasang di jaringan itu sendiri dan tidak mengganggu trafik jaringan yang dipantau. Perangkat keras itu bisa berupa *router* atau bisa *router gateway*, seperti yang diilustrasikan gambar 12.4.. Proses kerja NIDS sangat sederhana dengan melakukan *sniffs* (mengendus) interface perangkat internal *firewall* dalam mode *read-only*, sehingga dapat memantau ke dalam jaringan lalu lintas masuk dan keluar ke atau dari perangkat jaringan yang mencurigakan, yang kemudian mengirimkannya peringatan ke server Manajemen NIDS melalui antarmuka jaringan yang berbeda (Pandya, 2013).

Solusi NIDS menawarkan kemampuan deteksi intrusi *real-time* yang canggih, yang terdiri dari kumpulan komponen yang saling beroperasi: perangkat mandiri, sensor perangkat keras, dan komponen perangkat lunak yang umum. Ini bekerja bersama untuk

memungkinkan kemampuan deteksi intrusi jaringan yang lebih luas daripada solusi HIDS.

11.7 *Intrusion Detection System tools by Type Operating System*

Perushaan pengembang perangkat lunak IDS fokus terhadap implementasi aplikasinya masing-masing bedasarkan dari sistem operasi. Kebanyakan perangkat lunak IDS berbasiskan Unix, seperi Linux, maupun Mac OS. Namun, terdapat juga perangkat lunak IDS yang dikembangkan berbasiskan sistem operasi Windows. Tabel 12.1. di bawah ini menjelaskan beberapa platform sistem operasi yang mendukung instalasi aplikasi IDS yang berbasis *host* (HIDS), dan aplikasi IDS yang berbasis jaringan (NIDS).

Tabel 11.1. Jenis-Jenis Sistem Operasi yang Mendukung HIDS dan NIDS.

Nama	**IDS**		**Operating System**		
	Network	**Host**	**Linux**	**Windows**	**Mac**
Snort	Ya	-	√	√	-
OSSEC	-	Ya	√	√	√
CrowdSec	-	Ya	√	√	-
Suricata	Ya	-	√	√	√
Zeek	Ya	-	√	-	√
Sagan	Ya	Ya	√	-	√
Security Onion	Ya	Ya	√	-	-

Nama	IDS		Operating System		
	Network	Host	Linux	Windows	Mac
AIDE	-	Ya	√	-	√
OpenWIPS-NG	Ya	-	√	-	-
Samhain	-	Ya	√	-	√
Fail2Ban	-	Ya	√	-	√
Solar Wind	Ya	Ya	-	√	-
Manage Engine Event Log	-	Ya	√	√	√
Manage Engine Log 360	Ya	-	√	√	√

Daftar keterangan beberapa sistem operasi pada tabel 11.1 tersebut menganggap perangkat lunak sistem operasi yang kompatibel dengan aplikasi IDS jika dapat diinstal secara langsung.

DAFTAR PUSTAKA

Anderson, J. P. 1980. Computer Security Threat Monitoring and Surveillance. *Fort Washington*.

Ariyanto, A., & Asmunin. 2018. DETEKSI PAKET SNIFFING PADA WIRELLES MENGGUNAKAN ARP WATCH. *Jurnal Manajemen Informatika*, *8*(2), 178–181.

Conrad, E., Misenar, S., & Feldman, J. 2017. Domain 7. In *Eleventh Hour CISSP®* (pp. 145–183). Elsevier. https://doi.org/10.1016/B978-0-12-811248-9.00007-3

Direktorat Operasi Keamanan Siber. 2022. *Laporan Tahunan Monitoring Keamanan Siber 2022* (2022nd ed.). Direktorat Operasi Keamanan Siber - Indonesia Security Incident Response Team On Internet Infrastructure Coordination Center. https://bssn.go.id/monitoring-keamanan-siber-2022/

Khadafi, S., Meilani, B. D., & Arifin, S. 2017. Sistem Keamanan Open Cloud Computing Menggunakan Menggunakan IDS (Intrusion Detection System) Dan IPS (Intrusion Prevention System). *Jurnal IPTEK*, *21*(2), 67–76. https://doi.org/10.31284/j.iptek.2017.v21i2.207

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. 2019. Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada FTP Server Berbasiskan Linux Ubuntu Server. *Jurnal Ilmiah NERO*, *4*(3), 181–188. http://dx.doi.org/10.21107/nero.v4i3.137

Lin, Y., Zhang, Y., & Ou, Y.-J. 2010. The Design and Implementation of Host-Based Intrusion Detection System. *2010 Third International Symposium on Intelligent Information Technology and Security Informatics*, 595–598. https://doi.org/10.1109/IITSI.2010.127

Mansyur, A. R. 2020. Dampak COVID-19 Terhadap Dinamika Pembelajaran Di Indonesia. *Education and Learning Journal*, *Vol. 1, No*, 113–123.

Pandya, P. 2013. Chapter e16—Local Area Network Security. In J. R. Vacca (Ed.), *Computer and Information Security Handbook (Third Edition)* (pp. e1–e20). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-803843-7.00016-8

Varal, A. S., & Wagh, S. K. 2018. Misuse and Anomaly Intrusion Detection System using Ensemble Learning Model. *2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE)*, 1722–1727. https://doi.org/10.1109/ICRIEECE44171.2018.9009147

BAB 12
ADHOC NETWORKING

Oleh Agung Susilo Yuda Irawan

12.1 Pendahuluan

Dalam era digital yang semakin maju, keamanan informasi menjadi semakin penting. Salah satu aspek keamanan informasi yang perlu diperhatikan adalah jaringan nirkabel atau wireless network. Adhoc networking adalah salah satu jenis jaringan nirkabel yang sering digunakan dalam lingkungan bisnis dan pribadi. Adhoc networking memungkinkan perangkat untuk terhubung satu sama lain tanpa memerlukan akses poin atau router. Namun, keamanan adhoc networking sering menjadi perhatian karena adanya potensi ancaman keamanan dapat mengakibatkan kebocoran data atau serangan cyber. (Bakti Kominfo, 2021)

Bab 12 dari buku ini akan membahas tentang adhoc networking dan keamanannya. Bab ini akan membahas pengertian adhoc networking, teknik keamanan pada adhoc networking, protokol keamanan pada adhoc networking, manajemen keamanan pada adhoc networking, serta studi kasus tentang keamanan adhoc networking pada lingkungan perusahaan. Diharapkan dengan membaca bab ini, pembaca akan memahami pentingnya keamanan adhoc networking dan bagaimana cara mengimplementasikan keamanan pada adhoc networking.

12.2 Pengertian Adhoc Networking

Adhoc networking adalah jenis jaringan nirkabel yang memungkinkan perangkat untuk terhubung satu sama lain tanpa memerlukan akses poin atau router. Dalam jaringan adhoc, setiap

perangkat berfungsi sebagai node dan dapat berkomunikasi langsung dengan perangkat lain dalam jaringan. Jaringan adhoc sering digunakan dalam lingkungan bisnis dan pribadi karena mudah diatur dan tidak memerlukan infrastruktur jaringan yang kompleks.

Jaringan adhoc dapat digunakan dalam berbagai aplikasi, seperti jaringan kendaraan (VANET), jaringan seluler (MANET), dan jaringan sensor nirkabel (WSN). VANET adalah jaringan adhoc yang digunakan menghubungkan kendaraan dan memungkinkan komunikasi antara kendaraan atau antara kendaraan dan infrastruktur jalan. MANET adalah jaringan adhoc yang digunakan untuk menghubungkan perangkat seluler dan memungkinkan komunikasi antara perangkat tanpa memerlukan infrastruktur jaringan yang kompleks. WSN adalah jaring adhoc yang digunakan untuk menghubungkan sensor nirkabel dan memungkinkan pengumpulan data dari lingkungan yang diawasi.

Meskipun jaringan adhoc memiliki keuntungan dalam hal fleksibilitas dan kemudahan pengaturan, keamanan jaringan adhoc sering menjadi perhatian karena adanya potensi ancaman keamanan dapat mengakibatkan kebocoran data atau serangan cyber. Oleh karena itu, diperlukan teknik keamanan yang tepat untuk melindungi jaringan adhoc dari ancaman keamanan. (Trivusi, 2022)

12.3 Keamanan Adhoc Networking

Jaringan Adhoc adalah jaringan nirkabel yang terdiri dari beberapa perangkat yang terhubung satu sama lain tanpa memerlukan akses poin atau router. Jaringan Adhoc sering dig dalam kungan bisnis dan pribadi karena mudah diatur dan tidak memerlukan infrastruktur jaringan yang kompleks. Namun, keamanan jaringan Adhoc menjadi perhatian utama karena jaringan Adhoc rentan terhadap serangan keamanan. Ancaman keamanan pada jaringan Adhoc dapat berasal dari berbagai

sumber, seperti serangan *denial-of-service* (DoS), serangan *man-in-the-middle* (MITM), serangan jamming, dan serangan node jahat.

Untuk melindungi jaringan Adhoc dari ancaman keamanan, diperlukan teknik keamanan yang tepat. Beberapa teknik keamanan yang dapat digunakan pada jaringan Adhoc antara lain enkripsi data, autentikasi, dan manajemen kunci. Enkripsi data dapat digunakan untuk melindungi data yang dikirimkan dalam jaringan dari penyerangan MITM. Autentikasi dapat digunakan untuk memastikan bahwa perangkat yang terhubung ke jaringan adalah perangkat yang sah dan bukan perangkat yang mencurigakan. Manajemen kunci dapat digunakan untuk mengelola kunci enkripsi yang digunakan dalam jaringan. (Bakti Kominfo, 2021)

Beberapa penelitian telah dilakukan untuk mengatasi masalah keamanan pada jaringan Adhoc. Misalnya, penelitian oleh Kaur dan Singh (2016) membahas tentang masalah keamanan pada jaringan Adhoc dan teknik keamanan yang dapat digunakan untuk melindungi jaringan Adhoc dari serangan keamanan. Penelitian ini juga membahas tentang kelemahan teknik keamanan yang digunakan pada jaringan Adhoc dan tantangan dalam mengimplementasikan teknik keamanan pada jaringan Adhoc. Selain itu, penelitian oleh Al-Fuqaha *et al*. (2015) membahas tentang teknologi *Internet of Things* (IoT) dan tantangan keamanan yang terkait dengan penggunaan jaringan Adhoc dalam IoT. Penelitian ini juga membahas tentang teknik keamanan dapat digunakan untuk melindungi jaringan Adhoc dalam IoT. (Binus, 2017)

12.4 Ancaman Keamanan Pada Ahoc Networking

Serangan DoS adalah serangan yang bertujuan untuk membuat sumber daya jaringan tidak tersedia untuk pengguna yang sah dengan membanjiri jaringan dengan lalu lintas yang tidak perlu. Serangan MITM adalah serangan yang memungkinkan

penyerang untuk memantau atau memodifikasi komunikasi antara dua perangkat dalam jaringan. Serangan jamming adalah serangan yang mengganggu ketersediaan jaringan dengan mengirimkan sinyal yang mengganggu frekuensi jaringan. Serangan node jahat adalah serangan yang memungkinkan penyerang untuk mengambil alih kendali jaringan atau mengakses data yang dikirimkan dalam jaringan.

Untuk melindungi jaringan Adhoc dari ancaman keamanan, diperlukan teknik keamanan yang tepat. Beberapa teknik keamanan yang dapat digunakan pada jaringan Adhoc antara lain enkripsi data, autentikasi, dan manajemen kunci. Enkripsi data dapat digunakan untuk melindungi data yang dikirimkan dalam jaringan dari penyerangan MITM. Autentikasi dapat digunakan untuk memastikan bahwa perangkat yang terhubung ke jaringan adalah perangkat yang sah dan bukan perangkat yang mencurigakan. Manajemen kunci dapat digunakan untuk mengelola kunci enkripsi yang digunakan dalam jaringan.

Beberapa penelitian telah dilakukan untuk mengatasi masalah keamanan pada jaringan Adhoc. Misalnya, penelitian oleh Kaur dan Singh (2016) membahas tentang masalah keamanan pada jaringan Adhoc dan teknik keamanan yang dapat digunakan untuk melindungi jaringan Adhoc dari serangan keamanan. Penelitian ini juga membahas tentang kelemahan teknik keamanan yang digunakan pada jaringan Adhoc dan tantangan dalam mengimplementasikan teknik keamanan pada jaringan Adhoc. Selain itu, penelitian oleh Al-Fuqaha *et al.* (2015) membahas tentang teknologi *Internet of Things* (IoT) dan tantangan keamanan yang terkait dengan penggunaan jaringan Adhoc dalam IoT. Penelitian ini juga membahas tentang teknik keamanan dapat digunakan untuk melindungi jaringan Adhoc dalam IoT. (Al-Fuqaha, 2015)

12.5 Teknik Keamanan Pada Adhoc Networking

Jaringan Adhoc adalah jaringan nirkabel yang terdiri dari beberapa perangkat yang terhubung satu sama lain tanpa memerlukan akses poin atau router. Namun, jaringan Adhoc rentan terhadap serangan keamanan. Untuk melindungi jaringan Adhoc dari ancaman keamanan, diperlukan teknik keamanan yang tepat. Beberapa teknik keamanan yang dapatunakan pada jaringan Adhoc antara lain enkripsi data, autentikasi, dan manajemen kunci.

Enkripsi data adalah teknik keamanan yang digunakan untuk melindungi data yang dikirimkan dalam jaringan dari penyerangan MITM. Enkripsi data mengubah data yang dikirimkan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Autentikasi adalah teknik keamanan yang digunakan untuk memastikan bahwa perangkat yang terhubung ke jaringan adalah perangkat yang sah dan bukan perangkat yang mencurigakan. Autentikasi dapat dilakukan dengan menggunakan password atau sertifikat digital. Manajemen kunci adalah teknik keamanan yang digunakan untuk mengelola kunci enkripsi yang digunakan dalam jaringan. Manajemen kunci dapat dilakukan dengan menggunakan protokol kunci publik atau kunci simetris.

Beberapa penelitian telah dilakukan untuk mengatasi masalah keamanan pada jaringan Adhoc. Misalnya, penelitian oleh Kaur dan Singh (2016) membahas tentang masalah keamanan pada jaringan Adhoc dan teknik keamanan yang dapat digunakan untuk melindungi jaringan Adhoc dari serangan keamanan. Penelitian ini juga membahas tentang kelemahan teknik keamanan yang digunakan pada jaringan Adhoc dan tantangan dalam mengimplementasikan teknik keamanan pada jaringan Adhoc. Selain itu, penelitian oleh Al-Fuqaha *et al.* (2015) membahas tentang teknologi *Internet of Things* (IoT) dan tantangan keamanan yang terkait dengan penggunaan jaringan Adhoc dalam IoT. Penelitian ini juga membahas tentang teknik keamanan dapat digunakan untuk melindungi jaringan Adhoc dalam IoT.

12.6 Protokol Keamanan

Protokol keamanan pada jaringan Adhoc adalah serangkaian aturan dan prosedur yang digunakan untuk melindungi jaringan Adhoc dari ancaman keamanan. Protokol keamanan pada jaring Adhoc mencakup autentikasi, enkripsi, manajemen kunci, dan pengaturan kebijakan keamanan. Protokol keamanan yang tepat dapat membantu melindungi jaringan Adhoc dari serangan keamanan seperti serangan *denial-of-service* (DoS), serangan *man-in-the-middle* (MITM), serangan jamming, dan serangan node jahat. (Stall, 2017)

Autentikasi adalah proses untuk memastikan bahwa perangkat yang terhubung ke jaringan Adhoc adalah perangkat yang sah dan bukan perangkat yang mencurigakan. Autentikasi dapat dilakukan dengan menggunakan password atau sertifikat digital. Enkripsi adalah proses untuk mengubah data yang dikirimkan dalam jaringan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Enkripsi dapat dilakukan dengan menggunakan algoritma enkripsi seperti *Advanced Encryption Standard* (AES) atau *Rivest-Shamir-Adleman* (RSA). Manajemen kunci adalah proses untuk mengelola kunci enkripsi yang digunakan dalam jaringan. Manajemen kunci dapat dilakukan dengan menggunakan protokol kunci publik atau kunci simetris. Pengaturan kebijakan keamanan adalah proses untuk menentukan aturan dan prosedur yang harus diikuti oleh perangkat yang terhubung ke jaringan Adhoc.(S. K. Singh, 2016)

Beberapa protokol keamanan yang digunakan pada jaringan Adhoc antara lain *Transport Layer Security* (TLS), *Secure Shell* (SSH), dan *Internet Protocol Security* (IPsec). TLS adalah protokol keamanan yang digunakan untuk melindungi komunikasi antara perangkat dalam jaringan Adhoc. SSH adalah protokol keamanan yang digunakan untuk mengamankan akses jarak jauh ke perangkat dalam jaringan Adhoc. IPsec adalah protokol

keamanan yang digunakan untuk melindungi lalu lintas IP dalam jaringan Adhoc. (A. K. Pathan, 2009)

12.7 WEP (*Wired Equivalent Privacy*)

WEP (*Wired Equivalent Privacy*) adalah protokol keamanan yang digunakan pada jaringan nirkabel untuk melindungi data yang dikirimkan dalam jaringan. WEP menggunakan algoritma enkripsi RC4 untuk mengubah data yang dikirimkan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Namun, WEP memiliki kelemahan keamanan yang signifikan dan mudah diretas oleh penyerang.(S. S. Yerima, 2014)

Salah satu kelemahan WEP adalah penggunaan kunci enkripsi yang lemah. WEP menggunakan kunci enkripsi 40-bit atau 104-bit yang mudah diretas oleh penyerang dengan menggunakan teknik brute-force atau serangan lainnya. Selain itu, WEP juga rentan terhadap serangan *man-in-the-middle* (MITM) dan serangan replay. Serangan MITM memungkinkan penyerang untuk memantau atau memodifikasi komunikasi antara dua perangkat dalam jaringan, sed serangan replay memungkinkan penyerang untuk merekam dan memutar ulang lalu lintas jaringan. (H. Vargas-Hernández, 2018)

Sebagai hasil dari kelemahan keamanan WEP, protokol ini telah digantikan oleh protokol keamanan yang lebih kuat seperti WPA (Wi-Fi *Protected Access*) dan WPA2. WPA dan WPA2 menggunakan algoritma enkripsi yang lebih kuat dan memiliki fitur keamanan tambahan seperti autentikasi dan manajemen kunci yang lebih baik.

12.8 WPA (*Wi-fi Protected Acces*)

WPA (*Wi-Fi Protected Access*) adalah protokol keamanan yang digunakan pada jaringan nirkabel untuk melindungi data yang dikirimkan dalam jaringan. WPA menggunakan algoritma enkripsi TKIP (*Temporal Key Integrity Protocol*) untuk mengubah

data yang dikirimkan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Selain itu, WPA juga memiliki fitur keamanan tambahan seperti autentikasi dan manajemen kunci yang lebih baik dibandingkan dengan WEP. (D. A. Marchany and S. J. Radack, 2006)

Autentikasi pada WPA dapat dilakukan dengan menggunakan dua metode yaitu *Pre-Shared Key* (PSK) dan *Extensible Authentication Protocol* (EAP). PSK adalah metode autentikasi yang menggunakan password yang sama untuk semua perangkat yang terhubung ke jaringan. Sedangkan EAP adalah metode autentikasi yang menggunakan sertifikat digital untuk memastikan bahwa perangkat yang terhubung ke jaringan adalah perangkat yang sah.

Manajemen kunci pada WPA dilakukan dengan menggunakan protokol 4-way handshake. Protokol 4-way digunakan untuk menghasilkan kunci enkripsi yang unik untuk setiap sesi komunikasi antara perangkat dalam jaringan. Kunci enkripsi yang dihasil oleh protokol 4-way handshake lebih kuat dan lebih sulit diretas oleh penyerang. (R. L. Panko and J., 2015)

WPA telah digantikan oleh WPA2 yang menggunakan algoritma enkripsi yang lebih kuat yaitu *Advanced Encryption Standard* (AES). Namun, WPA masih digunakan pada beberapa jaringan nirkabel yang lebih lama dan tidak mendukung WPA2.

12.9 WPA2 (*Wi-fi Protected Acces* 2)

WPA2 (*Wi-Fi Protected Access* II) adalah protokol keamanan yang digunakan pada jaringan nirkabel untuk melindungi data yang dikirimkan dalam jaringan. WPA2 algoritma enkripsi *Advanced Encryption Standard* (AES) untuk mengubah data yang dikirimkan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Selain itu, WPA2 juga memiliki fitur keamanan tambahan seperti autentikasi dan manajemen kunci yang lebih baik dibandingkan dengan WPA. (Arana, 2006)

Autentikasi pada WPA2 dapat dilakukan dengan menggunakan dua metode yaitu *Pre-Shared Key* (PSK) dan *Extensible Authentication Protocol* (EAP). PSK adalah metode autentikasi yang menggunakan password yang sama untuk semua perangkat yang terhubung ke jaringan. Sedangkan EAP adalah metode autentikasi yang menggunakan sertifikat digital untuk memastikan bahwa perangkat yang terhubung ke jaringan adalah perangkat yang sah. (Sakib, 2011)

Manajemen kunci pada WPA2 dilakukan dengan menggunakan protokol 4-way handshake. Protokol 4-way digunakan untuk menghasilkan kunci enkripsi yang unik untuk setiap sesi komunikasi antara perangkat dalam jaringan. Kunci enkripsi yang dihasil oleh protokol 4-way handshake lebih kuat dan lebih sulit diretas oleh penyerang.

WPA2 adalah protokol keamanan yang paling umum digunakan pada jaringan nirkabel saat ini. Namun, WPA2 juga memiliki kelemahan keamanan seperti serangan brute-force pada password dan serangan *denial-of-service* (DoS). Oleh karena itu, diperlukan tindakan keamanan tambahan seperti penggunaan password yang kuat dan pemantauan lalu lintas jaringan untuk melindungi jaringan nirkabel dari serangan keamanan. (H. Vargas-Hernández, 2018)

12.10 Manajemen Keamanan Pada Adhoc Networking

Manajemen keamanan pada Adhoc Networking adalah serangkaian prosedur dan teknik yang digunakan untuk melindungi jaringan Adhoc dari ancaman keamanan. Manajemen keamanan pada Adhoc Networking mencakup autentikasi, enkripsi, manajemen kunci, dan pengaturan kebijakan keamanan. Manajemen keamanan yang tepat dapat membantu melindungi jaringan Adhoc dari serangan keamanan seperti serangan *denial-of-*

service (DoS), serangan *man-in-the-middle* (MITM), serangan jamming, dan serangan node jahat.

Autentikasi adalah proses untuk memastikan bahwa perangkat yang terhubung ke jaringan Adhoc adalah perangkat yang sah dan bukan perangkat yang mencurigakan. Autentikasi dapat dilakukan dengan menggunakan password atau sertifikat digital. Enkripsi adalah proses untuk mengubah data yang dikirimkan dalam jaringan menjadi bentuk yang tidak dapat dibaca oleh penyerang. Enkripsi dapat dilakukan dengan menggunakan algoritma enkripsi seperti *Advanced Encryption Standard* (AES) atau *Rivest-Shamir-Adleman* (RSA). Manajemen kunci adalah proses untuk mengelola kunci enkripsi yang digunakan dalam jaringan. Manajemen kunci dapat dilakukan dengan menggunakan protokol kunci publik atau kunci simetris. Pengaturan kebijakan keamanan adalah proses untuk menentukan aturan dan prosedur yang harus diikuti oleh perangkat yang terhubung ke jaringan Adhoc.

Beberapa protokol keamanan yang digunakan pada jaringan Adhoc antara lain Transport Layer Security (TLS*), Secure Shell* (SSH), *dan Internet Protocol Security* (IPsec). TLS adalah protokol keamanan yang digunakan untuk melindungi komunikasi antara perangkat dalam jaringan Adhoc. SSH adalah protokol keamanan yang digunakan untuk mengamankan akses jarak jauh ke perangkat dalam jaringan Adhoc IPsec adalah protokol keamanan yang digunakan untuk melindungi lalu lintas IP dalam jaringan Adhoc. (Alblwi, 2017)

12.11 Manajemen Identitas

Manajemen identitas pada Adhoc Networking adalah serangkaian prosedur dan teknik yang digunakan untuk mengelola identitas pengguna dan perangkat dalam jaringan Adhoc. Manajemen identitas pada Adhoc Networking mencakup autentikasi, otorisasi, dan manajemen identitas. Manajemen

identitas yang tepat dapat membantu melindungi jaringan Adhoc dari serangan keamanan seperti serangan *denial-of-service* (DoS), serangan *man-in-the-middle* (MITM), serangan jamming, dan serangan node jahat.

Autentikasi adalah proses untuk memastikan bahwa pengguna atau perangkat yang terhubung ke jaringan Adhoc adalah pengguna atau perangkat yang sah dan bukan pengguna atau perangkat yang mencurigakan. Autentikasi dapat dilakukan dengan menggunakan password atau sertifikat digital. Otorisasi adalah proses untuk memastikan bahwa pengguna atau perangkat yang terhubung ke jaringan Adhoc memiliki hak akses yang sesuai dengan peran dan tanggung jawab mereka dalam jaringan. Manajemen identitas adalah proses untuk mengelola informasi identitas pengguna dan perangkat dalam jaringan Adhoc. (D. A. Marchany and S. J. Radack, 2006)

Beberapa protokol keamanan yang digunakan pada jaringan Adhoc untuk manajemen identitas antara lain Kerberos, *Lightweight Directory Access Protocol* (LDAP), dan *Remote* Authentication Dial-In User Service (RADIUS). Kerberos adalah protokol keamanan yang digunakan untuk autentikasi dan otorisasi pengguna dalam jaringan Adhoc. LDAP adalah protokol keamanan yang digunakan untuk manajemen identitas pengguna dalam jaringan Adhoc. RADIUS adalah protokol keamanan yang digunakan untuk autentikasi dan otorisasi pengguna yang terhubung ke jaringan Adhoc melalui jaringan telepon. (R. L. Panko and J., 2015)

12.12 Manajemen Akses

Manajemen akses adalah salah satu teknik keamanan non-kriptografi pada jaringan adhoc yang digunakan untuk mengatur hak akses pengguna pada jaringan adhoc. Tujuan dari manajemen akses adalah untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses data yang dikirimkan melalui jaringan

adhoc. Manajemen akses meliputi pengaturan hak a pengguna, pengaturan kebijakan akses, dan pengaturan mekanisme autentikasi.

Pengaturan hak akses pengguna pada jaringan adhoc dilakukan dengan cara memberikan hak akses tertentu kepada pengguna yang terhubung ke jaringan adhoc. Hak akses yang diberikan dapat berupa hak akses penuh atau hak aksesbatas tergantung pada kebutuhan pengguna. Pengaturan kebijakan akses dilakukan dengan cara menentukan aturan-aturan yang harus diikuti oleh pengguna dalam mengakses data pada jaringan adhoc. Kebijakan akses dapat berupa aturan tentang jenis data yang dapat diakses, waktu akses, dan lokasi akses. Pengaturan mekanisme autentikasi dilakukan dengan cara memverifikasi identitas pengguna yang terhubung ke jaringan adhoc. Mekanisme autentikasi dapat berupa penggunaan username dan password atau penggunaan sertifikat digital. (D. A. Marchany and S. J. Radack, 2006)

Dalam penggunaan manajemen akses pada jaringan adhoc, perlu diperhatikan bahwa pengaturan hak akses yang terlalu ketat dapat menghambat produktivitas pengguna, sedangkan pengaturan hak akses yang terlalu longgar dapat membuka celah keamanan pada jaringan adhoc. Oleh karena itu, perlu dilakukan evaluasi dan pengembangan manajemen akses secara terus-menerus untuk menjaga keamanan pada jaringan adhoc. (R. L. Panko and J., 2015)

12.13 Manajemen Sertifikat

Manajemen sertifikat adalah salah satu teknik keamanan kriptografi pada jaringan adhoc yang digunakan untuk memastikan keaslian dan integritas data yang dikirimkanalui jaringan adhoc. Sertifikat digital digunakan untuk memverifikasi identitas pengguna dan memastikan bahwa data yang dikirimkan tidak diubah oleh pihak yang tidak berwenang. Manajemen sertifikat

meliputi pembuatan sertifikat digital, distribusi sertifikat digital, dan manajemen kunci publik.

Pembuatan sertifikat digital dilakukan dengan cara menghasilkan pasangan kunci publik dan kunci privat untuk setiap pengguna pada jaringan adhoc. Kunci publik digunakan untuk memverifikasi identitas pengguna, sedangkan kunci privat digunakan untuk mengenkripsi data yang dikirimkan. Distribusi sertifikat digital dilakukan dengan cara menyebarkan sertifikat digital ke setiap pengguna pada jaringan adhoc. Manajemen kunci publik dilakukan dengan cara mengelola kunci publik yang digunakan pada jaringan adhoc agar hanya pengguna yang sah yang dapat mengakses data yang dikirimkan. (D. A. Marchany and S. J. Radack, 2006)

Dalam penggunaan manajemen sertifikat pada jaringan adhoc, perlu diperhatikan bahwa penggunaan sertifikat digital yang tidak tepat dapat membuka celah keamanan pada jaringan adhoc. Oleh karena itu, perlu dilakukan evaluasi dan pengembangan manajemen sertifikat secara terus-menerus untuk menjaga keamanan pada jaringan adhoc.

12.14 Studi Kasus : Keamanan Adhoc Networking Pada Lingkungan Perusahaan

Keamanan jaringan adhoc pada lingkungan perusahaan menjadi semakin penting karena semakin banyak perusahaan yang menggunakan jaringan adhoc untuk memfasilitasi mobilitas karyawan dan akses ke perusahaan. Namun, jaringan adhoc memiliki risiko keamanan yang lebih tinggi dibandingkan dengan jaringan kabel karena sifatnya yang terbuka dan tidak terpusat. Oleh karena itu, perusahaan perlu mengimplementasikan teknik keamanan yang tepat untuk melindungi data perusahaan yang dikirimkan melalui jaringan adhoc.

Salah satu teknik keamanan yang dapat digunakan pada jaringan adhoc adalah teknik keamanan kriptografi. Teknik ini

meliputi enkripsi data, autentikasi, dan manajemen kunci. Enkripsi data digunakan untuk mengamankan data yang dikirimkan melalui jaringan adhoc dengan cara mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Autentikasi digunakan untuk memastikan bahwa pengguna yang terhubung ke jaringan adhoc adalah pengguna yang sah dengan cara memverifikasi identitas pengguna. Manajemen kunci digunakan untuk mengelola kunci enkripsi yang digunakan pada jaringan adhoc agar hanya pengguna yang sah yang dapat mengakses data yang dikirimkan.

Selain teknik keamanan kriptografi, teknik keamanan non-kriptografi juga dapat digunakan pada jaringan adhoc. Teknik ini meliputi deteksi intrusi, pemantauan jaringan, dan manajemen akses. Deteksi intrusi digunakan untuk mendeteksi serangan yang terjadi pada jaringan adhoc dengan cara memonitor aktivitas pada jaringan adhoc dan mendeteksi pola yang mencurigakan. Pemantauan jaringan digunakan untuk memantau aktivitas pada jaringan adhoc dan memastikan bahwa jaringan adhoc berjalan dengan baik. Manajemen akses digunakan untuk mengatur hak akses pengguna pada jaringan adhoc agar hanya pengguna yang sah yang dapat mengakses data yang dikirimkan. (Stall, W, 2017)
Dalam implementasi teknik keamanan pada jaringan adhoc pada lingkungan perusahaan, perlu dilakukan evaluasi dan pengembangan teknik keamanan secara terus-menerus untuk menjaga keamanan pada jaringan adhoc. Selain itu, perusahaan juga perlu melakukan pelatihan dan edukasi kepada karyawan mengenai pentingnya keamanan jaringan adhoc dan cara menggunakannya dengan aman.

Salah satu studi kasus mengenai keamanan jaringan adhoc pada lingkungan perusahaan adalah penelitian yang dilakukan oleh A. Al-Fuqaha, M. Guiz M. Mohammadi, M. Aledhari, dan M. Ayyash pada tahun 2015. Penelitian ini membahas tentang keamanan jaringan adhoc pada lingkungan *Internet of Things* (IoT) pada

perusahaan. Penelitian ini menunjukkan bahwa keamanan jaringan adhoc pada lingkungan perusahaan dapat ditingkatkan dengan menggunakan teknik keamanan kriptografi dan non-kriptografi seperti enkripsi data, autentikasi, manajemen kunci, deteksi intrusi, pemantauan jaringan, dan manajemen akses.

Selain itu, penelitian ini juga menunjukkan bahwa perusahaan perlu melakukan evaluasi dan pengembangan teknik keamanan secara terus-menerus untuk menjaga keamanan pada jaringan adhoc. Selain itu, perusahaan juga perlu melakukan pelatihan dan edukasi kepada karyawan mengenai pentingnya keamanan jaringan adhoc dan cara menggunakannya dengan aman.

12.15 Analisis Risiko

Analisis risiko adalah proses identifikasi, penilaian, dan pengendalian risiko yang terkait dengan suatu kegiatan atau proyek. Analisis risiko dilakukan untuk mengidentifikasiensi risiko yang dapat terjadi, mengevaluasi dampak dan kemungkinan terjadinya risiko, serta mengembangkan strategi pengendalian risiko yang tepat. Analisis risiko meliputi tiga tahap yaitu identifikasi risiko, penilaian risiko, dan pengendalian risiko. (H. Vargas-Hernández, 2018)

Tahap pertama dalam analisis risiko adalah identifikasi risiko. Pada tahap ini, dilakukan identifikasi potensi risiko yang dapat terjadi pada suatu kegiatan atau proyek. Identifikasi risiko dapat dilakukan dengan cara mengumpulkan informasi dari berbagai sumber, seperti pengalaman sebelumnya, data historis, dan wawancara dengan ahli terkait. Hasil dari tahap ini adalah daftar risiko yang teridentifikasi.

Tahap kedua dalam analisis risiko adalah penilaian risiko. Pada tahap ini, dilakukan penilaian terhadap dampak dan kemungkinan terjadinya risiko yang telah teridentifikasi pada tahap sebelumnya. Penilaian risiko dapat dilakukan dengan

menggunakan metode-metode tertentu, seperti analisis kuantitatif dan kualitatif. Hasil dari tahap ini adalah daftar risiko yang telah dinilai dan diberi prioritas berdasarkan dampak dan kemungkinan terjadinya risiko.

Tahap ketiga dalam analisis risiko adalah pengendalian risiko. Pada tahap ini, dilakukan pengembangan strategi pengalian risiko yang tepat untuk mengurangi dampak dan kemungkinan terjadinya risiko. Strategi pengendalian risiko dapat berupa penghindaran risiko, mitigasi risiko, transfer risiko, atau penerimaan risiko. Hasil dari tahap ini adalah rencana pengendalian risiko yang telah dikembangkan.

12.16 Implementasi Keamanan Pada Adhoc Networking

Implementasi keamanan pada adhoc networking adalah suatu proses untuk memastikan keamanan data yang dikirimkan melalui jaringan adhoc. Implementasi keamanan pada adhoc networking meliputi beberapa teknik keamanan, seperti enkripsi data, autentikasi, manajemen kunci, deteksi intrusi, pemantauan jaringan, dan manajemen akses.

Teknik keamanan pertama yang dapat digunakan pada adhoc networking adalah enkripsi data. Enkripsi data digunakan untuk mengamankan data yang dikirimkan melalui jaringan adhoc dengan cara mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Teknik keamanan kedua adalah autentikasi. Autentikasi digunakan untuk memastikan bahwa pengguna yang terhubung ke jaringan adhoc adalah pengguna yang sah dengan cara memverifikasi identitas pengguna. Teknik keamanan ketiga adalah manajemen kunci. Manajemen kunci digunakan untuk mengelola kunci enkripsi yang digunakan pada jaringan adhoc agar hanya pengguna yang sah yang dapat mengakses data yang dikirimkan.

Teknik keamanan selanjutnya adalah deteksi intrusi. Deteksi intrusi digunakan untuk mendeteksi serangan yang terjadi pada jaringan adhoc dengan cara memonitor aktivitas pada jaringan adhoc dan mendeteksi pola yang mencurigakan. Teknik keamanan lainnya adalah pemantauan jaringan. Pemantauan jaringan digunakan untuk memantau aktivitas pada jaringan adhoc dan memastikan bahwa jaringan adhoc berjalan dengan baik. Terakhir, teknik keamanan adalah manajemen akses. Manajemen akses digunakan untuk mengatur hak akses pengguna pada jaringan adhoc agar hanya pengguna yang sah yang dapat mengakses data yang dikirimkan. (Paridudin, 2021)

12.17 Evaluasi Keamanan Pada Adhoc Networking

Evaluasi keamanan pada adhoc networking adalah suatu proses untuk mengevaluasi keamanan jaringan adhoc yang telah diimplementasikan. Evaluasi keamanan pada adhoc networking meliputi beberapa tahap, seperti pengumpulan data, analisis data, dan pengembangan rekomendasi.

Tahap pertama dalam evaluasi keamanan pada adhoc networking adalah pengumpulan data. Pada tahap ini, dilakukan pengumpulan data mengenai keamanan jaringan adhoc yang telah diimplementasikan. Data yang dikumpulkan dapat berupa data historis, data pengguna, dan data teknis.

Tahap kedua dalam evaluasi keamanan pada adhoc networking adalah analisis data. Pada tahap ini, dilakukan analisis terhadap data yang telah dikumpulkan pada tahap sebelumnya. Analisis data dilakukan untuk mengevaluasi keamanan jaringan adhoc yang telah diimplementasikan dan mengidentifikasi potensi risiko yang dapat terjadi pada jaringan adhoc.

Tahap terakhir dalam evaluasi keamanan pada adhoc networking adalah pengembangan rekomendasi. Pada tahap ini, dilakukan pengembangan rekomendasi untuk meningkatkan keamanan jaringan adhoc yang telah diimplementasikan.

Rekomendasi yang dikembangkan dapat berupa pengembangan teknik keamanan yang lebih baik, pelatihan dan edukasi kepada pengguna jaringan adhoc, atau pengembangan kebijakan keamanan yang lebih ketat. (Pradana, P.D. , 2017)

DAFTAR PUSTAKA

Bakti Kominfo. 2021. Jaringan Ad Hoc: Jaringan Wireless dengan Biaya Rendah yang Bisa Anda Coba. https://www.baktikominfo.id/id/informasi/pengetahuan/jaringan_ad_hoc_jaringan_wireless_dengan_biaya_rendah_yang_bisa_anda_coba-810

Binus Malang. 2017. of Mobile Ad Hoc Network (MANET). https://binus.ac.id/malang/2017/09/introduction-of-mobile-ad-hoc-network-manet/

Trivusi. 2022. Mobile Adhoc Network. https://www. trivusi.web.id/2022/08/mobile-adhoc-network.html

Kaur, A., & Singh, S. 2016. A survey on security issues in mobile ad hoc networks. International Journal of Computer Applications, 139(3), 1-6. https://doi.org/10.5120/ijca2016910199

Al-Fuqaha, A., Guizani,., Mohammadi, M., Aledhari, M., & Ayyash, M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

https://doi.org/10.1109/COMST.2015.2444095.

Stall, W. 2017. Cryptography and network security: principles and practice. Pearson.

S. K. Singh and M. Singh, "A Survey on Ad Hoc Network Security," International Journal of Computer Science and Information Security, vol. 14, no. 1, pp. 1-7, 2016.

A. K. Pathan, H. Wang, and M. Li, "Security in Ad Hoc Networks: A General Overview," in Security in Ad Hoc and Sensor Networks, Springer, 2009, pp. 1-22.

S. S. Yerima, A. A. Gwandu, and A. A. Mohammed, "A Survey of Access Control in Ad Hoc Networks," International Journal of Computer Applications, vol. 97, no. 6, pp. 1-7, 2014.

H. Vargas-Hernández, "Risk Analysis and Management," in Encyclopedia of Information Science and Technology, Fourth Edition, IGI Global, 2018, pp. 1-14.
D. A. Marchany and S. J. Radack, "Risk Analysis and Management," in Handbook of Information Security, Springer, 2006, pp. 1-20.
R. L. Panko and J. P. Ordóñez de Pablos, "Risk Analysis and Management," in Encyclopedia of Information Science and Technology, Third Edition, IGI Global, 2015, pp. 1-12.
Arana, P., 2006. Benefits and vulnerabilities of Wi-Fi protected access 2 (WPA2). Infs, 612, pp.1-6.
Sakib, A.N., Jaigirdar, F.T., Munim, M. and Akter, A., 2011. Security improvement of WPA 2 (Wi-Fi protected access 2). IJEST, 3(1).
Alblwi, S. and Shujaee, K., 2017. A survey on wireless security protocol WPA2. In Proceedings of the international conference on security and management (SAM) (pp. 12-17). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
Pariddudin, A. and Syawaludin, M., 2021. Penerapan Algoritma Rivest Shamir Adleman Untuk Meningkatkan Keamanan Virtual Private Network. Teknois: Jurnal Ilmiah Teknologi Informasi dan Sains, 11(2), pp.73-84.
Pradana, P.D., Negara, R.M. and Dewanta, F., 2017. Evaluasi Performansi Protokol Routing DSR dan AODV Pada Simulasi Jaringan Vehicular Ad-Hoc Network (VANET) Untuk Keselamatan Transportasi Dengan Studi Kasus Mobil Perkotaan. eProceedings of Engineering, 4(2).

BAB 13
MOBILE ADHOC NETWORKING

Oleh Jarwo

13.1 *Mobile Ad Hoc Networking* (MANET)

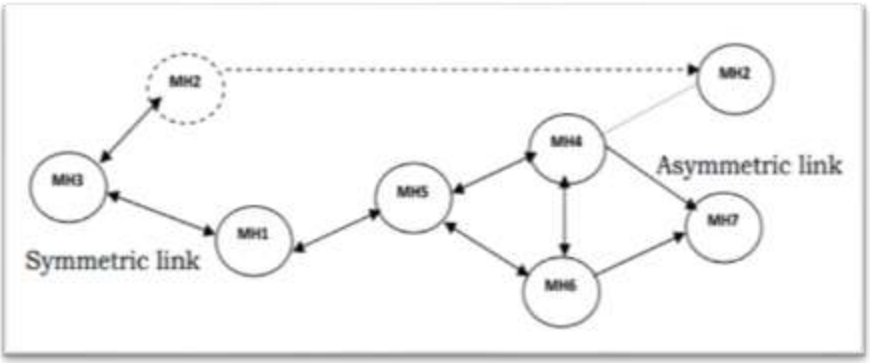
MANET adalah singkatan dari Mobile Ad Hoc Network, yang merupakan jaringan nirkabel yang terdiri dari beberapa perangkat yang dapat bergerak secara mandiri dan berkomunikasi satu sama lain tanpa memerlukan infrastruktur jaringan yang tetap atau titik akses sentral. Dalam MANET, setiap perangkat dapat berperan sebagai sumber, router, atau tujuan data, dan dapat berpindah tempat atau bergabung atau keluar dari jaringan kapan saja tanpa mengganggu komunikasi lainnya.

Jaringan MANET dapat terdiri dari beberapa jenis perangkat, seperti laptop, smartphone, sensor, kendaraan, dan drone. MANET sering digunakan dalam situasi-situasi di mana infrastruktur jaringan tetap tidak tersedia, terlalu mahal, atau tidak dapat diandalkan, seperti dalam operasi militer, penyelamatan bencana, atau dalam lingkungan industri yang bergerak cepat (Loo, *et al.*, 2016).

Dalam protokol MANET, antara node yang berbeda bisa terkoneksi melalui transmisi nirkabel secara langsung, akan tetapi bila salah satu node di luar jangkauan transmisi maka harus menentukan node lain untuk meneruskan pesan. Untuk alas an itulah, muncul skenario multi hop, yang mengondisikan beberapa host yang berfungsi sebagai relay dengan tugas meneruskan paket dari host sumber menuju kepada host tujuan.

MANET dapat dimodifikasi sesuai dengan kebutuhan, karena pada dasarnya minimal butuh dukungan dari

infrastruktur yang telah settle. Antar node terkoneksi sebagai jaringan adhoc sebagai sistem otonom dari mobile hosts (MH) yang berperan sebagai router dan terkoneksi memakai jaringan nirkabel. Hal ini berlawanan dengan jaringan seluler hop tunggal yang memerlukan BTS sebagai akses poin (Sarkar, *et al.*, 2007).



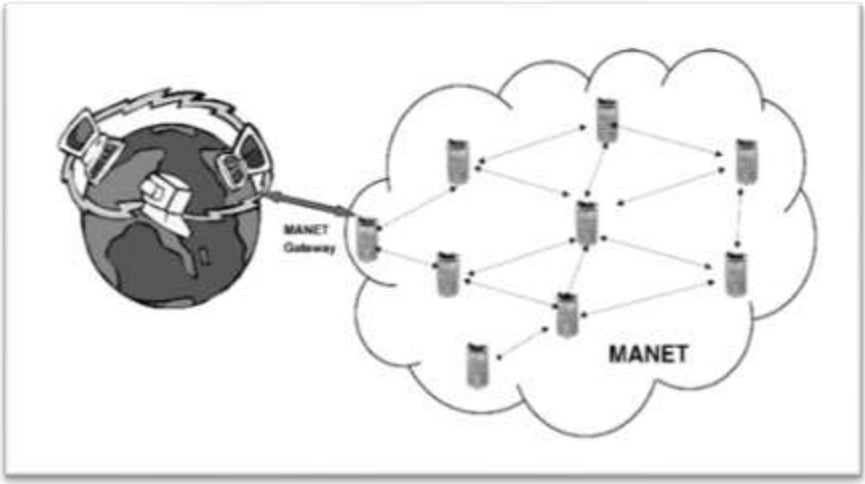
Gambar 13.1. Ilustrasi konektivitas jaringan MANET
Sumber: https://binus.ac.id/malang/2017/09/introduction-of-mobile-ad-hoc-network-manet/

Namun, MANET juga memiliki beberapa tantangan, seperti keamanan, skalabilitas, keterbatasan daya baterai, dan pergerakan perangkat yang dinamis, yang membuat desain dan implementasi jaringan yang efektif menjadi tantangan yang menantang.

13.2 Karakteristik MANET

Dalam dokumen *Request for Comments* dari *Mobile Ad Hoc Network*, dideskripsikan bahwa MANET terdiri dari peranti dasar bergerak seperti misalnya router dan peranti *nirkabel*). Dalam konteks ini "*node*" bebas bergerak ke mana saja. *Node* tersebut bisa berada di kendaraan bermotor, pesawat terbang, kapal laut, mobil dan dimanapun. Setiap *node* dilengkapi dengan peranti pemancar

dan penerima secara nirkabel, sehingga memungkinkan untuk dikombinasikan dari dengan peranti lain dan membentuk topologi MANET (Basagni, *et al.*, 2013).



Gambar 13.2. Topologi MANET
Sumber: https://media.wiley.com/product_data/excerpt/83/11180872/1118087283-83.pdf

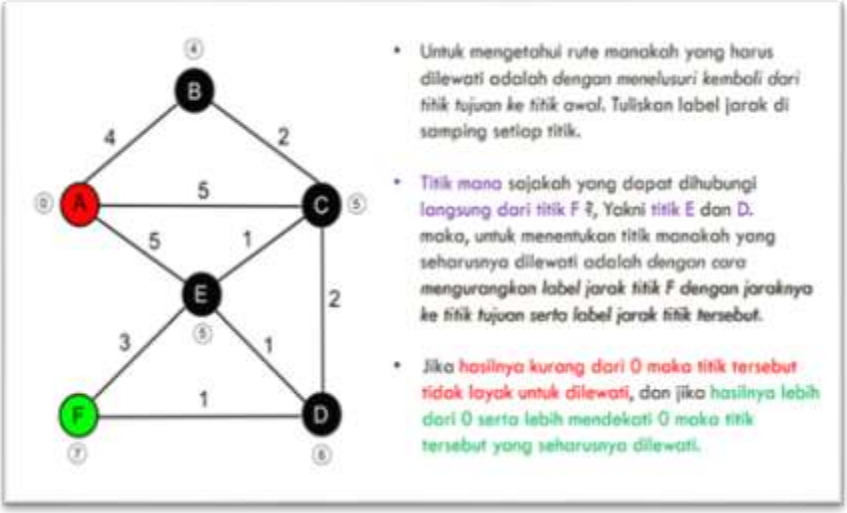
Secara umum, karakteristik utama dari MANET adalah sebagai berikut (Loo, *et al.,* 2016):

1. Desentralisasi: MANET tidak memiliki infrastruktur tetap, sehingga setiap perangkat dapat bertindak sebagai router dan mengirimkan informasi ke perangkat lain di jaringan.
2. Mobilitas: Setiap perangkat di MANET dapat bergerak secara bebas, sehingga jaringan harus dapat menyesuaikan diri dengan perubahan topologi jaringan.
3. Kapasitas jaringan terbatas: MANET biasanya memiliki kapasitas jaringan terbatas, karena perangkat yang terhubung biasanya memiliki sumber daya yang terbatas seperti daya baterai, memori, dan prosesor.

4. Keamanan yang lemah: MANET rentan terhadap serangan jaringan, karena tidak memiliki infrastruktur pusat dan tidak ada sistem keamanan yang dapat diandalkan.
5. Jangkauan jaringan yang terbatas: Jarak antar perangkat dalam MANET terbatas, sehingga jaringan biasanya digunakan untuk komunikasi antar perangkat yang berada di dekat satu sama lain.
6. Konfigurasi otomatis: MANET harus dapat mengkonfigurasi dirinya secara otomatis, karena tidak ada administrator jaringan yang dapat melakukan tugas tersebut.
7. Kecepatan transfer data yang beragam: Kecepatan transfer data dalam MANET dapat bervariasi tergantung pada jarak dan kualitas koneksi antara perangkat yang terhubung.

13.3 Protokol Routing pada MANET

Pada dasarnya Mobile Ad-hoc Network adalah jaringan nirkabel yang terdiri dari kombinasi besar perangkat mobile yang bergerak secara random dan tidak terstruktur. Dalam MANET, protocol routing digunakan untuk mengatur dan mengarahkan lalu lintas data antara node dalam jaringan. Protokol routing adalah aturan atau algoritma yang digunakan untuk menentukan rute yang optimal untuk mengirim data dari satu node ke node lain dalam jaringan (Basagni, *et al.,* 2013).



Gambar 13.3. Algoritma SPF (*Short Path First*), sebuah pendekatan protocol routing
Sumber: https://bongga.dosen.ittelkom-pwt.ac.id/wp-content/uploads/sites/57/2018/06/internetworking6.pdf

Ada beberapa protokol routing yang digunakan dalam MANET, di antaranya (Manapa, *et al.*, 2020):

1. *Proactive routing protocol*: Protokol ini melakukan pemetaan jaringan secara terus-menerus untuk memastikan bahwa setiap node memiliki informasi yang lengkap tentang jaringan. Contoh protokol ini adalah OLSR (*Optimized Link State Routing*) dan DSDV (*Destination Sequenced Distance Vector).*
2. Reactive routing protocol: Protokol ini hanya mengirimkan informasi rute ketika ada permintaan dari node yang ingin mengirimkan data. Contoh protokol ini adalah AODV (*Ad-hoc On-demand Distance Vector*) dan DSR (*Dynamic Source Routing*).

3. *Hybrid routing protocol*: Protokol ini menggabungkan karakteristik protokol proactive dan reactive. Protokol ini mengirimkan informasi rute secara teratur seperti pada *protokol proactive*, tetapi juga merespon permintaan *rute* dari node yang ingin mengirimkan data seperti pada *protokol reactive*. Contoh protokol ini adalah ZRP (*Zone Routing Protocol*).

Setiap protokol routing memiliki kelebihan dan kelemahan tersendiri, tergantung pada kondisi jaringan dan kebutuhan aplikasi. Oleh karena itu, pemilihan protokol routing yang tepat sangat penting untuk mencapai efisiensi dan keandalan dalam MANET.

13.4 Protokol DSDV

Protokol DSDV (*Destination-Sequenced Distance Vector*) adalah sebuah protokol routing pada jaringan komputer yang digunakan untuk mengirimkan data dari satu perangkat ke perangkat lainnya di dalam jaringan.

Mekanisme Protokol DSDV berdasarkan pada konsep algoritma routing vector jarak yang menggunakan tabel routing untuk menentukan jalur terbaik untuk pengiriman paket data.

Secara umum, mekanisme Protokol DSDV melibatkan dua tipe tabel routing: tabel routing dan tabel routing terkini. Tabel routing awalnya diisi dengan jalur yang diketahui oleh setiap node di dalam jaringan. Setiap node akan menyebar informasi tentang tabel routing-nya kepada node lainnya di jaringan (SEMARA PUTRA*, et al.,* 2016).

Ketika ada perubahan topologi jaringan atau keadaan lain yang dapat mempengaruhi pengiriman data, maka node akan memperbarui tabel routing terkininya dengan mengirim pesan berisi informasi tentang perubahan tersebut kepada node lain di dalam jaringan. Setelah itu, node tersebut akan menentukan jalur

terbaik untuk mengirimkan data dan menyimpan informasi tersebut pada tabel routing terkininya.

Dalam Protokol DSDV, setiap entri pada tabel routing terdiri dari beberapa informasi, seperti:

1. Destination: tujuan dari paket data
2. Next Hop: node berikutnya untuk pengiriman paket data
3. Sequence Number: nomor urut paket data
4. Metric: biaya untuk mengirim paket data ke tujuan

Ketika sebuah node ingin mengirimkan data ke node lain di dalam jaringan, maka node tersebut akan memeriksa tabel routing terkininya untuk menentukan jalur terbaik untuk mengirimkan data. Node tersebut akan mengirimkan data tersebut ke node berikutnya di jalur tersebut, dan seterusnya hingga sampai ke tujuan.

Protokol DSDV juga menggunakan mekanisme pencatatan nomor urut paket (*sequence number*) untuk menghindari terjadinya routing loop atau pengiriman data berulang. Setiap kali sebuah node mengirimkan informasi tentang tabel routing-nya ke node lain di dalam jaringan, node tersebut akan menambahkan nomor urut paket yang lebih besar dari nomor urut paket sebelumnya. Hal ini memastikan bahwa setiap node di dalam jaringan memiliki informasi routing yang paling mutakhir dan terkini.

Mekanisme Protokol DSDV melibatkan beberapa langkah berikut (Loo, *et al.,* 2016):

1. Setiap node dalam jaringan akan menyebar informasi tentang jaringan ke node tetangganya melalui paket hello.
2. Setiap node akan membuat tabel routing sendiri, yang berisi informasi tentang semua node dalam jaringan dan jalur terbaik ke setiap node.

3. Setiap baris dalam tabel routing terdiri dari beberapa informasi, termasuk tujuan node, nomor urut, jumlah loncatan, dan arah jalur.
4. Nomor urut pada setiap baris tabel routing adalah nomor urut yang diberikan kepada setiap paket yang diterima oleh node. Nomor urut ini membantu mencegah masalah loopback dan memastikan bahwa setiap node memiliki informasi routing yang paling akurat.
5. Setiap node secara periodik mengirimkan tabel routing ke semua node tetangganya. Setiap node juga mengirimkan tabel routing baru hanya jika ada perubahan dalam topologi jaringan.
6. Jika terjadi perubahan topologi, node akan memperbarui tabel routingnya dan mengirimkan informasi ini ke node tetangganya.
7. Setiap node akan memilih jalur terbaik ke tujuan dengan mempertimbangkan jumlah loncatan yang dibutuhkan dan nomor urut yang terbaru.

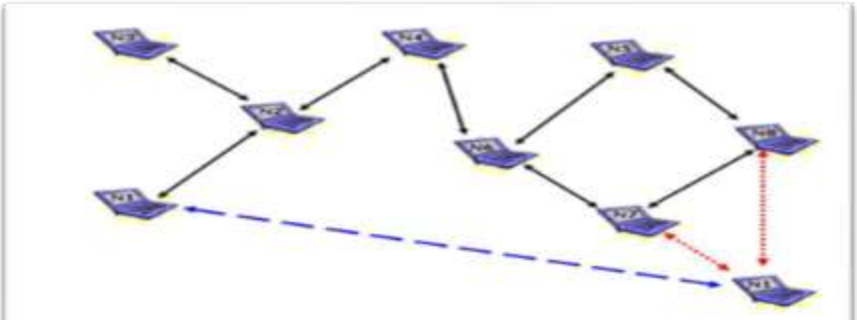


Figure 1. A network illustrating the movement of node N1

Table 1

The Routing table at Node 4

Destination	Metric	Sequence number
N1	2	S406-N2
N2	1	S128-N2
N3	2	S564-N2
N4	0	S710-N4
N5	2	S392-N6
N6	1	S076-N6
N7	2	S128-N6
N8	3	S050-N6

Table 2

The Routing table updated for Node 4

Destination	Metric	Sequence number
N1	3	S516-N6
N2	1	S238-N2
N3	2	S674-N2
N4	0	S820-N4
N5	2	S502-N6
N6	1	S186-N6
N7	2	S238-N6
N8	3	S160-N6

Gambar 13.4. Ilustrasi Mekanisme Protokol DSDV
Sumber: https://mti.binus.ac.id/2014/08/15/destination-sequenced-distance-vector-routing-dsdv/

Dengan mekanisme ini, Protokol DSDV memastikan bahwa setiap node memiliki informasi routing yang akurat dan up-to-date tentang seluruh jaringan, dan dapat merespon perubahan topologi dengan cepat. Namun, protokol ini juga menghasilkan overhead yang lebih besar karena setiap node harus secara periodik mengirim pesan routing ke tetangganya.

13.5 Protokol DSR

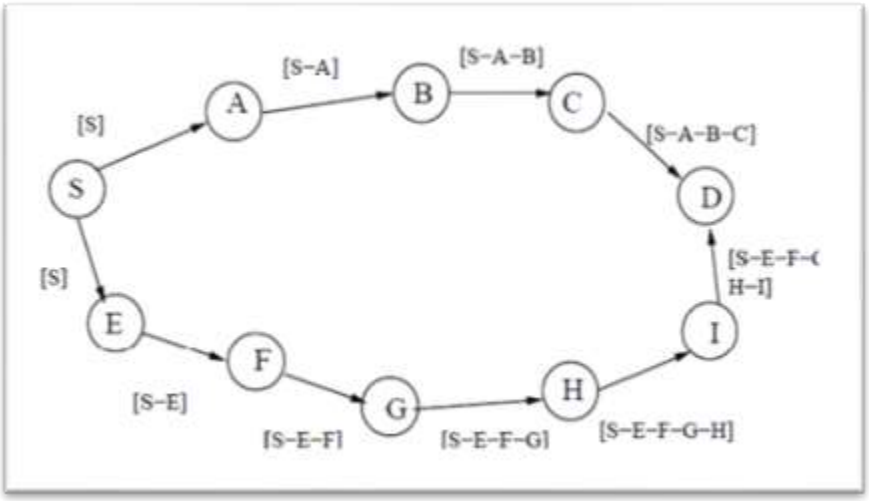
Protokol DSR (*Dynamic Source Routing*) adalah protokol routing yang digunakan dalam jaringan nirkabel ad-hoc, yang memungkinkan setiap node dalam jaringan untuk berperan sebagai router.

Mekanisme DSR bekerja dengan cara mengirimkan paket data dari node asal ke node tujuan secara langsung melalui rute yang ditentukan oleh paket itu sendiri. Dalam protokol DSR, setiap node dalam jaringan akan mempertahankan daftar node tetangga dan topologi jaringan, sehingga dapat menentukan rute terbaik untuk mengirimkan paket data ke tujuan (Anjani, 2021).

Paket data yang dikirimkan dalam protokol DSR akan membawa informasi header khusus yang berisi daftar node yang harus dilewati untuk mencapai tujuan. Jika node yang diperlukan untuk mencapai tujuan tidak ditemukan dalam daftar tetangga saat paket diterima, maka node akan mengirim permintaan route discovery ke node tetangga lainnya untuk mencari rute alternatif.

Saat menerima permintaan route discovery, node tetangga yang menerima permintaan tersebut akan mencari rute terbaik dan mengirimkan informasi rute kembali ke node yang meminta. Setelah menerima informasi rute, node asal akan memilih rute terbaik dan menambahkan informasi rute tersebut ke dalam header paket data.

Mekanisme DSR juga memungkinkan setiap node dalam jaringan untuk memperbarui daftar topologi jaringan secara dinamis saat ada perubahan pada topologi, misalnya ketika sebuah node baru bergabung dengan jaringan atau sebuah node keluar dari jaringan. Hal ini memungkinkan protokol DSR untuk menentukan rute terbaik yang selalu diperbarui dan beradaptasi dengan perubahan topologi jaringan secara real-time (Loo, *et al.,* 2016).



Gambar 13.5. Penjelajahan rute Protokol DSR
Sumber: https://www.researchgate.net/figure/Route-discovery-of-DSR-protocol_fig2_281460316

Protokol Dynamic Source Routing (DSR) adalah protokol routing tanpa pemetaan terpusat yang digunakan pada jaringan ad hoc (MANET) untuk mengirimkan data dari sumber ke tujuan. DSR bekerja dengan cara mengirimkan pesan berbasis permintaan dan respons, di mana setiap node memelihara cache informasi tentang rute yang ditemukan selama proses ini. Berikut adalah mekanisme DSR yang lebih rinci (Olivia Kembuan, 2014):

1. *Discovery Route*
   a. Node sumber mengirimkan pesan permintaan rute (*route request,* RREQ) ke node tetangga.
   b. Jika node tetangga memiliki informasi tentang rute ke tujuan, node tersebut akan mengirimkan pesan respons rute (*route reply*, RREP) ke node sumber.

c. Jika node tetangga tidak memiliki informasi tentang rute ke tujuan, node tersebut akan mengirimkan pesan RREQ ke node tetangga selanjutnya, dan proses ini berlanjut sampai rute ke tujuan ditemukan.
d. Selama proses ini, setiap node yang menerima pesan RREQ akan memasukkan informasi tentang rute ke dalam cache-nya.

2. Pengiriman Data
   a. Setelah rute ditemukan, node sumber mengirimkan data ke node tujuan.
   b. Setiap node yang menerima data akan memeriksa cache-nya untuk menentukan apakah ada informasi tentang rute ke tujuan. Jika ada, node tersebut akan mengirimkan data ke node selanjutnya dalam rute tersebut. Jika tidak ada, node tersebut akan mengirimkan pesan RREQ untuk mencari rute baru.

3. Perawatan Cache
   a. Setiap node mempertahankan cache informasi tentang rute yang ditemukan selama proses discovery route.
   b. Setiap cache mencakup informasi tentang rute, seperti alamat node sumber, node tujuan, dan node selanjutnya dalam rute.
   c. Cache ini diperbarui secara dinamis saat informasi rute berubah atau saat node tetangga bergabung atau meninggalkan jaringan.

13.6 Protokol ZRP

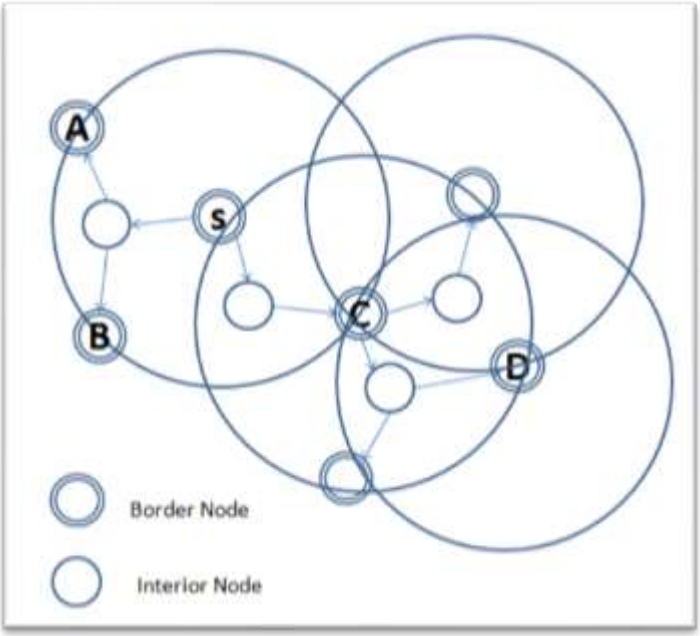
Protokol ZRP (*Zone Routing Protocol*) adalah protokol routing yang digunakan dalam jaringan ad hoc. Tujuan utamanya adalah untuk meningkatkan efisiensi routing dengan mengurangi overhead kontrol pesan di jaringan.

Mekanisme Protokol ZRP terdiri dari beberapa bagian (Halid, 2023):

1. Zoning: Jaringan dibagi menjadi beberapa zona dengan menggunakan algoritma clustering. Setiap zona terdiri dari beberapa simpul yang saling terhubung. Setiap simpul di jaringan harus tergabung dalam setidaknya satu zona.
2. *Intra-zone routing*: Setiap zona memiliki protokol routing sendiri untuk mengarahkan lalu lintas antara simpul di dalam zona itu. IARP bertanggung jawab untuk routing di dalam zona, yang terdiri dari sekelompok node yang saling terhubung secara langsung. Setiap node dalam zona mengumpulkan informasi topologi dari node tetangganya dan membuat tabel routing lokal. Ketika sebuah paket dikirimkan dari satu node ke node lain dalam zona, node tersebut menggunakan tabel routing lokalnya untuk memilih rute terbaik. Jika tidak ada rute yang tersedia, node akan mengirimkan permintaan routing ke semua node dalam zona untuk mencari rute yang mungkin. Protokol routing yang digunakan untuk intra-zone routing dapat bervariasi tergantung pada kebutuhan jaringan.
3. *Inter-zone routing*: IERP bertanggung jawab untuk routing antar zona. Ketika sebuah paket harus dikirimkan ke node yang berada di luar zona, node akan menggunakan IERP untuk mencari rute terbaik. IERP bekerja dengan membuat topologi virtual dari jaringan yang disebut dengan routing zone. Setiap routing zone memiliki node yang disebut dengan gateway node yang berfungsi sebagai penghubung antar zona. Setiap node dalam routing zone mengirimkan informasi topologi ke gateway node, yang digunakan untuk membuat tabel routing global. Ketika sebuah paket dikirimkan ke node di luar zona, node akan menggunakan tabel routing global untuk mencari rute terbaik melalui gateway node. Ketika lalu lintas perlu bergerak di antara zona, protokol routing ZRP akan digunakan. Ada dua jenis inter-zone routing: reactive dan

proactive. Dalam reactive routing, pesan hanya dikirim ketika diperlukan, misalnya ketika rute baru diperlukan. Dalam proactive routing, informasi tentang semua rute antar zona diperbarui secara teratur, tanpa menunggu permintaan.

4. *Rute caching:* Protokol ZRP menggunakan mekanisme caching untuk mengurangi overhead routing. Setiap simpul menyimpan informasi tentang rute ke simpul lain yang baru-baru ini dikunjungi. Ketika lalu lintas harus diteruskan ke simpul yang sama, rute yang disimpan di cache dapat digunakan.



Gambar 13.6. Penjelajahan Rute Zone pada Protokol ZRP
Sumber: https://www.researchgate.net/figure/Zone-Routing-Protocol-ZRP_fig2_303318875

Dalam ringkasan, Protokol ZRP menggunakan algoritma zoning untuk membagi jaringan menjadi beberapa zona. Setiap zona memiliki protokol routing sendiri untuk mengarahkan lalu lintas antara simpul di dalam zona itu. Ketika lalu lintas perlu bergerak di antara zona, protokol routing ZRP akan digunakan. Protokol ZRP juga menggunakan caching untuk mengurangi overhead routing dan meningkatkan efisiensi jaringan.

DAFTAR PUSTAKA

Anjani, M. &. N. H., 2021. Pengaruh Pergerakan Node Pada Protokol Routing Dynamic Manet On Demand (DYMO) Dalam Mobile Ad-Hoc Network (MANET). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 5(1), pp. 105-114.

Basagni, S., Conti, M., Giordano, S. & Stojmenovic, I., 2013. *Mobile Ad Hoc Networking: Cutting Edge Directions.* 2 ed. s.l.:Wiley-IEEE Press.

Halid, A. L. O. J. T. &. M. F., 2023. DYNAMIC MANET ON DEMAND PROTOCOL PADA JARINGAN SENSOR NIRKABEL UNTUK SISTEM MONITORING LAHAN PERTANIAN. *ILKOM Jurnal Ilmiah,* 9(2), pp. 211-217.

Loo, J., Mauri, J. L. & Ortiz, J. H., 2016. *Mobile Ad Hoc Networks: Current Status and Future Trends.* 1 ed. Boca Raton: CRC Press.

Manapa, E. S., Sampetoding, E. A. M. & Lewakabessy, G., 2020. POTENSI PENGGUNAAN MOBILE AD-HOC NETWORK (MANET) SEBAGAI ALAT KOMUNIKASI DATA PADA TRANSPORTASI DI INDONESIA. *Dinamic Saint Journal,* 4(2), p. 865–868.

Olivia Kembuan, W. &. S. S. K., 2014. Analisis Kinerja Reactive Routing Protocol dalam Mobile Ad-Hoc Network (MANET) Menggunakan NS-2 (Network simulator). *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi,* 1(1), pp. 1-7.

Reddy, G. R. M. & M, K., 2017. *Mobile Ad Hoc Networks: Bio-Inspired Quality of Service Aware Routing Protocols.* 1 ed. Boca Raton: CRC Press.

Sarkar, S. K., Basavaraju, T. G. & Puttamadappa, C., 2007. *Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications.* 1 ed. Boca Raton: CRC Press.

SEMARA PUTRA, I. G. N., DIAFARI DJUNI H, I. G. & SUDIARTA, P. K., 2016. ANALISA KINERJA MANET (Mobile Ad Hoc Network) PADA LAYANAN VIDEO CONFERENCE DENGAN RESOLUSI YANG BERBEDA. *Jurnal SPEKTRUM,* 3(2), pp. 15-20.

BIODATA PENULIS

Angga Aditya Permana
Dosen Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Nur Hayati, S.Si., MTI
Dosen Program Studi Informatika
Fakultas Teknologi Komunikasi dan Informatika

Penulis lahir di Jakarta tanggal 16 Juni 1984. Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional. Menyelesaikan pendidikan S1 pada Jurusan Matematika, Universitas Nasional dan S2 pada Jurusan Magister Teknologi Informasi, Universitas Indonesia serta sedang menempuh program studi S3 pada jurusan Ilmu Komputer, Institut Pertanian Bogor. Pernah mendapatkan hibah dikti terkait dengan bidang Kriptografi dan mendapatkan sertifikasi internasional FCCH (Foresec Certified in Computer Hacking) serta sudah menerbitkan beberapa jurnal terkait dengan penerapan dan analisis pada bidang Kriptografi.

BIODATA PENULIS

Abdurrasyid, S.Kom., MMSI.
Dosen Program Studi Teknik Informatika
Fakultas Telematika Energi Institut Teknologi PLN

Penulis lahir di Jakarta tanggal 10 Juni 1987. Saat ini penulis menjadi dosen tetap pada Program Studi Teknik Informatika, Fakultas Telematika Energi, Institut Teknologi PLN Jakarta. Penulis aktif melakukan publikasi dalam berbagai jurnal ilmiah baik nasional maupun internasional dapat diakses pada link ini, memiliki ketertarikan pada bidang software engineering dan machine learning, dan saat ini penulis sedang melanjutkan studinya di Institut Teknologi Bandung.

BIODATA PENULIS

Rima Rizqi Wijayanti, S.ST., MMSI.
Dosen Program Studi Teknik Informatika
Fakultas Teknik, Universitas Muhammadiyah Tangerang

Penulis lahir di Jakarta tanggal 22 Mei 1986. Saat ini penulis merupakan dosen tetap pada Program Studi Teknik Informatika Fakultas Teknik, Universitas Muhammadiyah Tangerang. Penulis menyelesaikan pendidikan S1 di STMI Jakarta dan melanjutkan S2 di Universitas Gunadarma pada Tahun 2017, serta memiliki ketertarikan pada bidang sistem informasi.

BIODATA PENULIS

Marniyati H. Botutihe, S.Kom., M.Kom
Dosen Program Studi Sistem Informasi
Fakultas Ilmu Komputer Universitas Pohuwato

Penulis lahir di Parigi tanggal 07 Oktober 1990. Penulis adalah dosen tetap pada Program Studi Sistem Operasi Fakultas Ilmu Komputer, Universitas Pohuwato. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Teknik Informatika.

BIODATA PENULIS

Dr. Irmawati, S.Kom., MMSI.
Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 dan S2 pada Program Studi Sistem Informasi Universitas Gunadarma dan S3 pada departemen Teknik Elektro Universitas Indonesia. Penulis menekuni bidang keilmuan meliputi *Artificial Intelligence*, *Image Processing*, *Machine Learning*, dan *Deep Learning*.

BIODATA PENULIS

Iwan Adhicandra, S.T., M.Sc.
Dosen Program Studi Informatika
Universitas Bakrie

Penulis adalah dosen tetap pada Program Studi Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Bakrie. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro konsentrasi bidang Teknik Telekomunikasi di Universitas Trisakti dan melanjutkan S2 pada Jurusan Teknik Elektro konsentrasi bidang Komunikasi Data di University of Sheffield, Inggris. Penulis adalah Senior Member di Institute of Electrical and Electronic Engineers (SMIEEE).

BIODATA PENULIS

Yendi Putra, S. Kom., M. Kom, MTA
Dosen Program Studi Manajemen Informatika
Fakultas Eknomi Universitas Mahaputra Muhammad Yamin

Penulis lahir di Salimpaung pada tanggal 3 Januari 1988. Penulis merupakan anak kedua dari tiga bersaudara. Saat ini, penulis menjabat sebagai dosen tetap pada Program Studi Manajemen Informatika, Fakultas Ekonomi, Universitas Mahaputra Muhammad Yamin. Perjalanan pendidikan penulis dimulai pada tahun 2007, ketika penulis menyelesaikan pendidikan D1 di LKP Palapa Komputer Batusangkar. Tahun 2010, penulis melanjutkan pendidikan S1 Jurusan Sistem Informasi di STMIK Indonesia Padang. Kemudian, penulis melanjutkan studi pascasarjana dengan menempuh pendidikan Magister di Universitas Putra Indonesia (UPI YPTK-Padang) pada tahun 2018. Bidang teknologi, khususnya dalam keamanan, menjadi minat utama penulis. Selama studi S2, penulis menulis tesis dengan fokus pada penggunaan Algoritma Advanced Encryption Standard (AES) untuk meningkatkan keamanan token sebuah website dari serangan Cross-Site Scripting (XSS). Penulis memiliki pemahaman mendalam tentang berbagai aspek keamanan dan terus mengembangkan pengetahuannya

dalam bidang ini. Selain kegiatan akademik, penulis juga aktif dalam berbagai lomba di bidang komputer. Pada tahun 2022, penulis berhasil meraih juara ketiga pada ajang Lomba Kompetensi Keterampilan Instruktur Nasional (KKIN) Wilayah Barat yang diadakan di Banda Aceh. Partisipasi penulis dalam lomba-lomba ini menunjukkan dedikasi dan keahlian dalam bidang komputer. Penulis juga memiliki peran sebagai seorang orang tua. Penulis memiliki dua orang anak, yaitu Ayumna yang berusia 4 tahun dan Ibrahim yang berusia 8 bulan. Keluarga merupakan sumber inspirasi dan dukungan utama bagi penulis dalam mengejar karir akademik dan minatnya di bidang teknologi. Penulis merupakan individu yang berdedikasi, penuh semangat, dan memiliki minat khusus dalam bidang keamanan teknologi.

BIODATA PENULIS

Arief Yanto Rukmana, S.T., M.M.
Mahasiswa Doktoral Universitas Pendidikan Indonesia
Dosen Perguruan Tinggi Indonesia Mandiri Bandung
Dosen Universitas Nurtanio Bandung

Penulis sebelumnya telah memegang posisi penting di sejumlah bisnis yang beroperasi pada skala nasional dan dunia. penulis saat ini berprofesi sebagai praktisi bisnis (Pemilik Perusahaan di Bidang Fashion, Kuliner dan Bisnis Digital juga sebagai seorang akademisi. Penulis mengajar di Universitas Nurtanio Bandung, dan dosen tetap di perguruan tinggi indonesia mandiri (STMIK IM & STIE STAN IM). alumni dari Program Studi Informatika (S1) Sekolah Tinggi Manajemen Informatika dan Komputer Indonesia Mandiri (STMIK IM), Program Magister Manajemen (S2) di Pasca Sarjana Universitas Widyatama dan sedang melanjutkan studi Pendidikan (S3) Program Doktoral Pendidikan Teknologi dan Vokasional di Universitas Pendidikan Indonesia. Penulis aktif sebagai pembicara dan narasumber kewirausahaan digital juga berdedikasi sebagai praktisi bisnis / owner / pemilik beberapa perusahaan yang bergerak pada industri food, fashion and fun. serta aktif dalam organisasi nasional maupun internasional. Penulis juga seorang profesional dalam bidang public

speaking & sebagai asesor kompetensi digital dan instruktur berpengalaman untuk sertifikasi kompetensi SKKNI BNSP Digital Marketing, Social Media Marketing dan Metodologi Pelatihan Level III, Graphic Design serta Sertifikasi Kompetensi beberapa lainnya yang diselenggarakan dinas tenaga kerja kota bandung, PT Rice INTI dan Balai Besar Pengembangan Latihan Kerja (BBPLK) Bandung. Selain itu pula penulis produktif sebagai pendamping UMKM dan pengelola Inkubator Bisnis Perguruan Tinggi Indonesia Mandiri dengan membina dan melatih / coaching, mentoring serta melakukan pendampingan bisnis UMKM / Start UP untuk mahasiswa yang berminat menjadi seorang Entrepreneur / Technopreneurship tangguh yang mampu berdayasaing pada kancah internasional.

BIODATA PENULIS

Suwito Pomalingo, S.Kom., M.Kom.
Dosen Program Studi Informatika Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktoral dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS

Shah Khadafi, S.Kom., M.Kom.
Dosen Program Studi Sistem Informasi
Fakultas Teknik Elektro dan Teknologi Informasi

Penulis lahir di Surabaya tanggal 28 september 1983. Penulis adalah dosen tetap pada Program Studi Sistem Informasi, Fakultas Teknik Elektro dan Teknologi Informasi, di Institut Teknologi Adhi Tama Surabaya (ITATS). Menyelesaikan pendidikan S1 pada Jurusan Sistem Komputer dan melanjutkan S2 pada Jurusan Teknologi Informasi. Penulis menekuni bidang keilmuan Jaringan Komputer, Keamanan Sistem Informasi dan Teknologi Informasi, Soft Computing, dan Travelling Salesman Problem.

BIODATA PENULIS

Agung Susilo Yuda Irawan, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang

Penulis lahir di Kuningan tanggal 15 Juni 1993. Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang . Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Magister Ilmu Komputer.

BIODATA PENULIS

Jarwo, ST, MM
Dosen Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Pomosda Nganjuk

Penulis lahir di Magetan pada tanggal 07 Mei 1981. Penulis adalah dosen tetap pada Program Studi Teknik Informatika Sekolah Tinggi Teknologi Pomosda Nganjuk. Menyelesaikan Pendidikan S1 Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Pomosda Nganjuk dan melanjutkan S2 pada Universitas Islam Kadiri Kediri pada jurusan Manajemen dengan konsentrasi Sistem Informasi Manajemen. Pada perguruan tinggi homebase, penulis mengampu mata kuliah Mata Kuliah Bahasa Otomata, Teknik Kompilasi, Matematika Diskrit, Kecerdasan Buatan, Keamanan Jaringan dan Mekatronika IOT. Penulis aktif dan tertarik pada bidang Pengelolaan Informasi, Decision Support System dan beberapa kajian khas pada Kecerdasan Buatan. Penulis dapat dihubungi melalui surat elektronik jarwosttpmd@gmail.com.