JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Evaluasi Sistem Keamanan Komputer: Analisis Ancaman, Kriptografi, dan Perlindungan Data Modern

Zul Fadly[1]*, Zulkarnaen Lubis[2], Dendy Rivaldo Alwisyah[3], Dedy Munandar[4], Muhammad Riski Afriyansyah[5]
[1,2,3,4,5] Universitas Malikussaleh, Indonesia
[1]zul.240170198@mhs.unimal.ac.id, [2]zulkarnaen.240170101@mhs.unimal.ac.id, [3]dendy.240170087@mhs.unimal.ac.id, [4]dedy.240170102@mhs.unimal.ac.id, [5]muhammad.240170081@mhs.unimal.ac.id

ABSTRACT

Computer security plays a crucial role in protecting the confidentiality, integrity, and availability of digital information in modern computing environments. This study evaluates key computer security components through an analysis of threat models, operating system security mechanisms, cryptographic approaches, and modern data protection techniques. The research reviews user management, firewall configuration, system updates, and layered defense strategies, as well as the characteristics and propagation of contemporary malware such as ransomware, spyware, and network-based attacks. Classical and modern cryptographic methods, hashing functions, digital signatures, and steganography are also examined as essential elements in ensuring secure information processing. Using a descriptive qualitative method supported by literature studies and system observations, the findings indicate that effective computer security requires a multilayered approach supported by consistent system maintenance and increased user awareness to mitigate evolving cyber threats.

Keywords: *computer security, cryptography, malware, firewall, steganography.*

PENDAHULUAN

Perkembangan teknologi informasi yang eksponensial telah mengubah paradigma operasional dunia secara fundamental. Komputer dan sistem digital kini bukan sekadar alat bantu, melainkan komponen kritis dalam infrastruktur vital, pengelolaan data perbankan, komunikasi pemerintahan, hingga operasional sektor pendidikan. Memasuki era Industri 4.0 dan transisi menuju Society 5.0, ketergantungan masyarakat terhadap integritas sistem digital semakin tinggi. Digitalisasi memang menawarkan efisiensi luar biasa dalam proses bisnis dan layanan publik, namun di sisi lain, ia membuka pintu bagi risiko keamanan yang semakin canggih dan merusak.

Ancaman siber tidak lagi didominasi oleh peretas amatir yang sekadar mencari pengakuan, melainkan telah berevolusi menjadi industri kriminal yang terorganisir. Fenomena seperti *Ransomware-as-a-Service* (RaaS), pencurian data berskala besar (*data breach*), dan rekayasa sosial (*social engineering*) berkembang pesat seiring dengan meluasnya konektivitas internet. Serangan-serangan ini menargetkan celah keamanan pada perangkat lunak, perangkat keras, hingga lapisan psikologis pengguna. Kerugian yang ditimbulkan tidak hanya bersifat finansial, tetapi juga mencakup kerusakan reputasi institusi dan hilangnya kepercayaan publik.

Keamanan sistem komputer modern menuntut pendekatan yang holistik. Mekanisme pertahanan tradisional yang hanya mengandalkan antivirus statis tidak lagi memadai untuk menahan serangan dinamis. Sistem operasi sebagai tulang punggung manajemen sumber daya komputer menjadi target utama eksploitasi, terutama jika pengelolaannya mengabaikan prinsip-prinsip dasar keamanan seperti pembaruan *patch* berkala dan konfigurasi hak akses yang ketat. Selain itu, aspek kriptografi memegang peranan vital dalam mengamankan data yang bergerak di jaringan publik. Penggunaan algoritma enkripsi mutakhir, fungsi hash untuk validasi integritas, serta tanda tangan digital untuk otentikasi menjadi standar wajib dalam menjaga kerahasiaan informasi. Penelitian ini bertujuan untuk mengevaluasi secara komprehensif mekanisme keamanan komputer, menganalisis evolusi ancaman siber terkini, serta merumuskan strategi perlindungan data yang efektif dalam menghadapi tantangan era digital.

TINJAUAN PUSTAKA

Tinjauan pustaka ini menguraikan landasan teori yang relevan mengenai arsitektur keamanan komputer, standar perlindungan informasi, karakteristik ancaman siber, serta perkembangan teknik kriptografi.

Prinsip Dasar Keamanan Informasi (CIA Triad)

Model keamanan informasi berpedoman pada kerangka kerja *Confidentiality, Integrity, and Availability* (CIA Triad). *Confidentiality* (kerahasiaan) menjamin bahwa informasi hanya dapat diakses oleh pihak yang memiliki otorisasi, yang diimplementasikan melalui enkripsi data dan mekanisme otentikasi biometrik atau *password*. *Integrity* (integritas) memastikan akurasi dan konsistensi data selama siklus hidupnya, mencegah modifikasi yang tidak sah

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

melalui penggunaan *checksum* dan fungsi hash kriptografis. *Availability* (ketersediaan) menjamin bahwa sistem dan data dapat diakses oleh pengguna yang sah kapan pun dibutuhkan, yang dicapai melalui redundansi perangkat keras, *load balancing*, dan proteksi terhadap serangan *Distributed Denial of Service* (DDoS).

Mekanisme Keamanan Sistem Operasi

Setiap sistem operasi memiliki arsitektur keamanan yang unik. Microsoft Windows menerapkan pendekatan berlapis melalui *Windows Defender*, *SmartScreen*, dan *User Account Control* (UAC) yang membatasi hak eksekusi aplikasi tanpa izin administrator. Namun, arsitektur Windows yang populer menjadikannya target utama malware, sehingga efektivitasnya sangat bergantung pada kedisiplinan pengguna dalam melakukan pembaruan sistem (*Windows Update*). Di sisi lain, sistem operasi berbasis Linux/Unix menggunakan model keamanan berbasis *permission* (rwx) yang ketat dan pemisahan *root user* yang jelas. Struktur ini secara inheren membatasi penyebaran virus, meskipun kesalahan konfigurasi oleh administrator tetap dapat membuka celah kerentanan. Pada platform mobile, Android dan iOS memanfaatkan teknik *sandboxing*, yang mengisolasi setiap aplikasi dalam ruang memori terpisah untuk mencegah akses data lintas aplikasi yang tidak sah.

Evolusi Malware dan Rekayasa Sosial

Lansekap ancaman siber didominasi oleh *malware* (perangkat lunak berbahaya). Ransomware mengenkripsi file korban menggunakan algoritma asimetris dan menuntut tebusan dalam bentuk *cryptocurrency*. Trojan menyamar sebagai perangkat lunak sah untuk memberikan akses pintu belakang (*backdoor*) kepada penyerang. Spyware bekerja secara senyap mengumpulkan data keystroke dan kredensial pengguna. Selain serangan teknis, rekayasa sosial (*social engineering*) seperti *phishing* memanipulasi psikologi manusia untuk menipu pengguna agar menyerahkan data sensitif secara sukarela. Studi literatur menegaskan bahwa faktor manusia sering kali menjadi "rantai terlemah" dalam sistem keamanan.

Kriptografi Modern

Kriptografi telah berkembang dari teknik substitusi klasik menjadi algoritma matematis kompleks. Kriptografi simetris (contoh: AES-256) menggunakan satu kunci untuk enkripsi dan dekripsi, sangat efisien untuk mengamankan data dalam jumlah besar. Kriptografi asimetris (contoh: RSA, ECC) menggunakan sepasang kunci (publik dan privat) untuk mengatasi masalah distribusi kunci dan memfasilitasi tanda tangan digital. Fungsi Hash (seperti SHA-256) digunakan untuk memverifikasi integritas file, di mana perubahan satu bit saja pada input akan menghasilkan *output* hash yang berbeda secara drastis, sehingga manipulasi data dapat dideteksi dengan segera.

METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur dan observasi sistem. Metode ini dipilih untuk memberikan pemahaman mendalam mengenai fenomena keamanan komputer yang kompleks dan dinamis.

Tahapan pengumpulan data dilakukan melalui dua sumber utama. Pertama, studi kepustakaan dilakukan dengan menganalisis jurnal ilmiah nasional dan internasional, buku teks standar keamanan (seperti karya Stallings dan Schneier), serta laporan tahunan ancaman siber dari vendor keamanan global. Referensi ini digunakan untuk memetakan tren serangan terbaru, seperti evolusi ransomware dan teknik eksploitasi *Zero-Day*. Kedua, observasi teknis dilakukan dengan mengamati implementasi fitur keamanan pada berbagai lingkungan sistem operasi (Windows 10 dan Ubuntu Linux 20.04 LTS). Observasi mencakup evaluasi konfigurasi *firewall*, efektivitas manajemen *patch*, serta respons sistem terhadap simulasi ancaman sederhana.

Analisis data dilakukan secara komparatif dan interpretatif. Analisis komparatif digunakan untuk membedakan efektivitas mekanisme keamanan bawaan antar sistem operasi serta membandingkan performa algoritma kriptografi klasik versus modern. Analisis interpretatif digunakan untuk menelaah pola serangan berdasarkan data statistik insiden, memahami motivasi di balik serangan siber, dan mengevaluasi peran faktor kesalahan manusia dalam keberhasilan serangan. Kesimpulan ditarik secara induktif untuk merumuskan rekomendasi strategi keamanan yang adaptif.

HASIL DAN PEMBAHASAN

Keamanan sistem komputer merupakan resultan dari interaksi antara teknologi proteksi, kebijakan manajemen, dan kesadaran pengguna. Temuan penelitian menunjukkan bahwa meskipun teknologi keamanan telah sangat maju, metode serangan juga berevolusi menjadi lebih canggih dan sulit dideteksi.

Analisis Tren dan Distribusi Ancaman Siber

Berdasarkan sintesis data dari berbagai laporan keamanan siber terkini, teridentifikasi distribusi jenis ancaman yang paling dominan menyerang infrastruktur TI organisasi maupun perangkat individu. Data ini menggambarkan

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

pergeseran fokus serangan dari sekadar perusakan (*vandalism*) menjadi aktivitas profitabel.

Berikut adalah tabel distribusi insiden ancaman siber yang menjadi fokus analisis:

Table 1. Distribusi Jenis Ancaman Siber Berdasarkan Frekuensi Insiden

Threat Type	Incidents (%)
Ransomware	35%
Spyware	20%
Trojan	18%
Worm	12%
Phishing	15%

Sebagaimana ditampilkan pada Table 1, Ransomware menempati peringkat tertinggi dalam frekuensi insiden. Untuk memberikan visualisasi yang lebih jelas mengenai proporsi ancaman ini, disajikan diagram batang berikut:

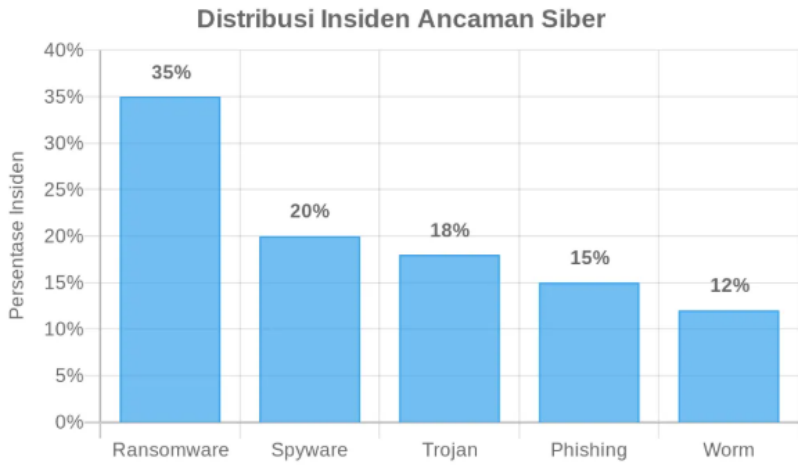

Fig. 1. Distribusi Insiden Ancaman Siber

Pembahasan Mendalam:

Mekanisme Serangan Mengacu pada Fig. 1, dominasi Ransomware (35%) menunjukkan tingkat bahaya yang kritis. Ransomware modern tidak hanya mengenkripsi data, tetapi juga menerapkan taktik *double extortion*, di mana penyerang mengancam akan membocorkan data curian ke publik jika tebusan tidak dibayar. Secara teknis, ransomware sering kali masuk melalui celah *Remote Desktop Protocol* (RDP) yang lemah atau lampiran email *phishing*.

Ancaman Spyware (20%) dan Trojan (18%) menunjukkan tren serangan persisten (*Advanced Persistent Threat* - APT). Malware jenis ini dirancang untuk bersembunyi selama mungkin di dalam jaringan korban guna mencuri kredensial perbankan, data kartu kredit, atau rahasia dagang perusahaan. Sementara itu, tingginya angka Phishing (15%) mengonfirmasi bahwa rekayasa sosial tetap menjadi vektor serangan yang efektif. Penyerang memanfaatkan manipulasi psikologis, seperti urgensi palsu atau penyamaran sebagai institusi resmi, untuk memancing korban mengklik tautan berbahaya.

Peran Kriptografi dan Tantangan IoT Dalam menghadapi ancaman tersebut, implementasi kriptografi menjadi benteng terakhir pertahanan data. Algoritma AES (Advanced Encryption Standard) dengan panjang kunci 256-bit saat ini dianggap sebagai standar emas untuk enkripsi data simpanan (*data at rest*). Namun, tantangan baru muncul pada era *Internet of Things* (IoT). Perangkat IoT sering kali memiliki sumber daya komputasi terbatas yang tidak mampu menjalankan algoritma kriptografi berat, menjadikannya titik masuk yang rentan bagi penyerang untuk menyusup ke jaringan utama. Oleh karena itu, pengembangan algoritma *Lightweight Cryptography* menjadi sangat krusial untuk mengamankan ekosistem perangkat cerdas.

Selain itu, penggunaan Digital Signature dan fungsi hash (SHA-256) mutlak diperlukan untuk menjamin integritas perangkat lunak. Tanpa verifikasi tanda tangan digital, pengguna berisiko menginstal pembaruan palsu yang telah disusupi malware (*supply chain attack*). Steganografi juga memberikan lapisan keamanan tambahan dengan menyembunyikan eksistensi pesan rahasia di dalam media digital, meskipun teknik ini harus digunakan dengan hati-hati agar tidak dimanfaatkan oleh aktor jahat untuk menyembunyikan komunikasi *Command and Control* (C2).

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Strategi Mitigasi Berbasis Defense in Depth Hasil penelitian merekomendasikan penerapan strategi *Defense in Depth* (pertahanan berlapis) yang komprehensif:

1. Pengamanan Jaringan: Implementasi *Next-Generation Firewall* (NGFW) dan sistem deteksi intrusi (IDS/IPS) untuk memfilter lalu lintas berbahaya secara *real-time*.
2. Pengerasan Sistem (System Hardening): Melakukan manajemen patch otomatis untuk menutup celah kerentanan Zero-Day, serta menerapkan prinsip Least Privilege di mana pengguna hanya diberikan hak akses minimal yang diperlukan.
3. Proteksi Data: Penerapan enkripsi menyeluruh (end-to-end encryption) baik saat data disimpan maupun ditransmisikan, serta strategi backup data rutin yang terisolasi dari jaringan utama (offline backup) untuk memitigasi dampak ransomware.
4. Edukasi Pengguna: Pelatihan kesadaran keamanan (Security Awareness) secara berkala untuk meningkatkan kemampuan pengguna dalam mendeteksi upaya phishing dan rekayasa sosial.

.KESIMPULAN

Penelitian ini menyimpulkan bahwa keamanan sistem komputer adalah entitas dinamis yang memerlukan adaptasi berkelanjutan terhadap lansekap ancaman yang terus berubah. Analisis mendalam menunjukkan bahwa kerentanan sistem modern bersifat multidimensi, tidak hanya bersumber dari cacat teknis perangkat lunak, tetapi juga sangat dipengaruhi oleh faktor perilaku manusia dan kebijakan manajemen yang lemah. Ransomware dan serangan berbasis rekayasa sosial teridentifikasi sebagai ancaman paling kritis yang memanfaatkan celah tersebut.

Keamanan yang efektif tidak dapat dicapai hanya dengan mengandalkan satu jenis teknologi. Diperlukan sinergi antara konfigurasi sistem operasi yang ketat, implementasi kriptografi standar industri (seperti AES dan RSA), serta mekanisme otentikasi yang kuat. Selain itu, aspek edukasi pengguna menjadi kunci vital; teknologi keamanan tercanggih sekalipun akan gagal jika pengguna dengan mudah menyerahkan kredensial mereka kepada penyerang melalui skema *phishing*.

Ke depan, organisasi dan individu disarankan untuk beralih dari pendekatan keamanan reaktif menuju proaktif. Penerapan arsitektur *Zero Trust*—di mana tidak ada entitas yang dipercaya secara implisit—serta pemantauan keamanan berkelanjutan menjadi prasyarat mutlak untuk membangun ketahanan digital yang tangguh. Integrasi antara perlindungan teknis, prosedur operasional yang disiplin, dan budaya sadar keamanan akan menciptakan ekosistem komputasi yang mampu bertahan menghadapi tantangan keamanan siber di masa depan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Malikussaleh atas dukungan fasilitas dan lingkungan akademis yang kondusif dalam penyusunan penelitian ini. Apresiasi mendalam juga disampaikan kepada para dosen pembimbing serta rekan-rekan mahasiswa yang telah memberikan kontribusi pemikiran, kritik konstruktif, dan referensi literatur yang sangat berharga selama proses penelitian berlangsung. Dukungan ini menjadi motivasi utama bagi penulis untuk menyelesaikan studi ini dengan baik.

REFERENSI

Bishop, M. (2019). *Computer Security: Art and Science* (2nd ed.). Addison-Wesley Professional.

Conti, M., Dragoni, N., & Lesyk, V. (2018). A Survey of Ransomware Prevention and Mitigation Solutions. *ACM Computing Surveys (CSUR)*, 51(1), 1–36. https://doi.org/10.1145/3214301

Ilham, D. N., Hardisal, H., Balkhaya, B., Candra, R. A., & Sipahutar, E. (2019). Heart Rate Monitoring and Stimulation with the Internet of Thing-Based (IoT) Alquran Recitation. *SinkrOn*, 4(1), 221. https://doi.org/10.33395/sinkron.v4i1.10392

Ilham, D. N., Satria, E., Anugreni, F., Candra, R. A., & Kusumo, H. N. R. A. (2021). Rain Monitoring System for Nutmeg Drying Based on Internet of Things. *Journal of Computer Networks, Architecture, and High-Performance Computing*, 3(1), 52–57. https://doi.org/10.47709/cnahpc.v3i1.933

Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press. https://doi.org/10.1201/9781351133036

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of Applied Cryptography*. CRC Press.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.

Richardson, R. (2021). Ransomware: The mounting threat to global cybersecurity. *Computer Fraud & Security*, 2021(11), 13–15. https://doi.org/10.1016/S1361-3723(21)00118-2

Schneier, B. (2017). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (20th Anniv. Ed.). Wiley.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 02, **Number** 01, Mei 2026

Sutherland, I., Read, H., & Xynos, K. (2018). Forensic Analysis of Ransomware Families. *Journal of Information Security and Applications*, 39, 1–12. https://doi.org/10.1016/j.jisa.2018.01.002

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.