JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Studi Literatur Terhadap Evolusi Virus Komputer: Mekanisme Penyebaran, Investigasi Forensik, dan Strategi Deteksi Berbasis Kecerdasan Buatan

Muhammad Ausid Addari[1*], Ghanda Ramadhan Siregar[2], Afriza Briliansyah Lubis[3], Cut Intan Ariestia[4], Zatalini[5]
[1,2,3,4,5] Program Studi Teknik Informatika, Universitas Malikussalaeh, Indonesia
[1]muhammad.240170123@mhs.unimal.ac.id, [2]ghanda.240170222@mhs.unimal.ac.id,
[3]afriza.240170218@mhs.unimal.ac.id, [4]cut.240170074@mhs.unimal.ac.id, [5]zatalini.240170116@mhs.unimal.ac.id

ABSTRACT

The escalation of post-pandemic malware threats has surpassed the capacity of conventional defenses, as social engineering techniques and code manipulation have become primary infiltration instruments exploiting vulnerabilities in user behavior and system structures. This study aims to analyze the evolution of malware propagation techniques, evaluate the effectiveness of digital forensic investigations, and test the robustness of artificial intelligence-based detection methods. Employing a Systematic Literature Review (SLR) approach toward case studies and algorithmic experiments from the 2023–2025 period, this research synthesizes data from real-world attack investigations and machine learning model performances. The results indicate that while algorithms such as Decision Trees and Ensemble Learning offer high accuracy, their effectiveness is increasingly compromised by adversarial attacks capable of deceiving AI logic. Furthermore, forensic findings in ransomware cases confirm that aggressive encryption speeds necessitate a shift in mitigation strategies from post-incident analysis to proactive hybrid defenses. This study concludes that the integration of behavioral detection technology and systemic resilience through data backup management is the primary key to countering the mutation of contemporary cyber threats.

Keywords:
Malware, Artificial Intelligence, Digital Forensics, Ransomware, Mitigation.

PENDAHULUAN

Perkembangan teknologi digital yang pesat saat ini ternyata diikuti oleh risiko keamanan yang tidak kalah cepat pertumbuhannya. Masalahnya bukan sekadar pada teknologinya, melainkan pada bagaimana ancaman tersebut seringkali tidak disadari oleh para pengguna. Sebagai contoh, hasil penelitian menunjukkan bahwa meskipun 90% mahasiswa merasa sudah paham mengenai bahaya *phishing* (Wahyu Hidayat M et al., 2023), namun pada kenyatannya banyak yang masih terjebak oleh teknik manipulasi psikologis. Hal ini menunjukkan adanya ketimpangan antara rasa percaya diri pengguna dengan realitas serangan di lapangan, di mana malware seperti *njRAT* masih sangat efektif menyebar melalui teknik rekayasa sosial (Rizky et al., 2016).

Selain faktor manusia, sistem pertahanan teknis kita juga menghadapi tantangan besar. Metode keamanan tradisional yang hanya mengandalkan daftar virus yang sudah dikenal (*signature-based*) kini mulai dianggap kurang efektif dalam menangani virus-virus baru yang kodenya terus berubah-ubah (Tiana et al., 2025). (Kristian et al., 2025) menyarankan perlunya strategi mitigasi yang lebih menyeluruh, namun pendekatan ini seringkali sulit diterapkan jika tidak dibantu oleh teknologi yang lebih pintar seperti kecerdasan buatan. Memang, penggunaan Big Data dijanjikan mampu membantu proses deteksi (Tiana et al., 2025), tetapi kita juga harus realistis terhadap kendala biaya dan kerumitan perangkat yang dibutuhkan untuk menjalankannya.

Kondisi pasca-pandemi yang memaksa semua aktivitas berpindah ke dunia digital telah menciptakan banyak celah keamanan baru (Karunia et al., 2025). Isu utamanya adalah virus-virus modern saat ini tidak lagi hanya merusak file, tetapi sudah mampu mempelajari cara kerja sistem agar tidak terdeteksi. Jurnal ini mencoba mengkaji bagaimana cara menghadapi ancaman tersebut, dengan batasan khusus pada perangkat berbasis Windows dan Android. Melalui penggabungan data dari investigasi nyata dan teknologi kecerdasan buatan, pendahuluan ini ingin menekankan bahwa sistem keamanan yang kuat harus menggabungkan antara kecanggihan algoritma dengan kehati-hatian penggunanya.

TINJAUAN PUSTAKA

Menganalisis taksonomi ancaman siber saat ini menuntut pemahaman mendalam mengenai arsitektur malware yang semakin kompleks. Secara teknis, perbedaan antara virus konvensional dan *worm* terletak pada mekanisme replikasinya; di mana *worm* memanfaatkan celah pada protokol jaringan untuk melakukan penggandaan diri secara otonom tanpa memerlukan interaksi pengguna (Sumarno, 2023). Namun, pandangan tradisional yang mengandalkan pembaruan basis data antivirus (murwodo, 2023) kini menghadapi tantangan besar. Riset terbaru menunjukkan bahwa efektivitas deteksi berbasis tanda tangan (*signature-based*) menurun drastis ketika berhadapan dengan teknik

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

obfuscation tingkat tinggi, seperti polimorfisme dan metamorfisme, yang secara dinamis mengubah struktur biner malware untuk menghindari pemindaian statis (Tiana et al., 2025).

Evolusi ini mencapai puncaknya pada serangan *ransomware* modern seperti Ryuk, yang mengintegrasikan kemampuan enkripsi tingkat tinggi di lingkungan *cloud* dengan kecepatan eksekusi yang sangat agresif (Kusuma, 2023). Hal yang sering luput dari kajian teknis umum adalah bagaimana infiltrasi ini seringkali memanfaatkan penyalahgunaan panggilan API (*Application Programming Interface*) yang sah untuk melakukan operasi file yang destruktif (Hartinah et al., 2023). Sementara banyak literatur masih memfokuskan analisis pada sistem operasi Android melalui evaluasi izin aplikasi (Aura Jelita & Siregar, 2025), terdapat celah pengetahuan yang cukup besar mengenai bagaimana evolusi serupa terjadi pada sistem *embedded* atau perangkat *legacy* yang tidak mendukung agen keamanan modern.

Di sisi lain, adopsi algoritma cerdas seperti *Decision Tree* dan *Ensemble Learning* telah menjadi standar baru dalam klasifikasi malware berdasarkan fitur-fitur biner dan perilaku (Aditya Pratama & Murdiansyah, 2025). Namun, kita harus kritis terhadap dependensi model AI ini. (Andi Novianto, 2025) memberikan catatan teknis penting mengenai munculnya serangan *adversarial*, di mana penyerang sengaja menyuntikkan *noise* atau memanipulasi fitur masukan sehingga model klasifikasi cerdas salah dalam mengenali *payload* berbahaya sebagai file aman. Oleh karena itu, tinjauan ini menegaskan bahwa masa depan pertahanan siber tidak hanya terletak pada kecanggihan algoritma, tetapi pada kemampuan sistem untuk mengolah anomali dalam struktur Big Data secara *real-time* guna menutupi kelemahan analisis statis konvensional.

METODE PENELITIAN

Memilih metodologi untuk membedah evolusi malware sering kali memaksa kita berada di persimpangan antara kedalaman analisis perilaku atau keluasan cakupan data. Jurnal ini tidak bermaksud melakukan eksperimen laboratorium secara terisolasi, melainkan menerapkan pendekatan Systematic Literature Review (SLR) sebagai instrumen untuk menguji validitas tren keamanan siber dalam rentang tahun 2023 hingga 2025. Proses berpikir di balik pemilihan SLR ini didasarkan pada kebutuhan untuk melihat pola besar (meta-pola) serangan siber pasca-pandemi yang tidak mungkin tertangkap hanya melalui satu uji coba perangkat lunak. Namun, kita harus kritis terhadap metode ini: risiko terbesar SLR adalah potensi bias pada basis data jurnal yang hanya mempublikasikan hasil-hasil sukses, sehingga penelitian ini secara sadar melakukan triangulasi data dengan membandingkan hasil investigasi forensik nyata (Kusuma, 2023) terhadap model teoritis yang ditawarkan oleh algoritma deteksi terbaru (Tiana et al., 2025).

Dalam memilah sumber, penelitian ini menerapkan kriteria inklusi yang ketat, memprioritaskan studi yang menyajikan data kuantitatif terkait akurasi deteksi dan durasi enkripsi. Kontras yang tajam sering terjadi pada perbandingan antara analisis statis dan dinamis. Sementara (Adenansi & A. Novarina, 2017) berargumen bahwa analisis dinamis memberikan gambaran utuh melalui pemantauan runtime, riset terbaru dari (Tiana et al., 2025) justru menunjukkan bahwa analisis dinamis mulai kewalahan menghadapi adversarial attacks yang dirancang untuk mendeteksi keberadaan sandbox. Oleh sebab itu, kerangka kerja penelitian ini disusun untuk tidak hanya memvalidasi klaim efisiensi algoritma, tetapi juga mempertanyakan ketahanannya dalam lingkungan yang tidak ideal. Strategi pencarian literatur difokuskan pada tiga pilar utama: mekanisme infiltrasi (seperti API calls), model klasifikasi cerdas (Machine Learning), dan teknik respons insiden (Live Forensics).

Penting untuk diakui secara jujur bahwa metodologi ini memiliki keterbatasan spesifik pada ketergantungan terhadap aksesibilitas dokumentasi teknis dari vendor keamanan siber yang sering kali bersifat tertutup (proprietary). Hal ini membatasi analisis pada malware yang sudah teridentifikasi atau masuk dalam dataset publik. Selain itu, fokus pada platform Windows dan Android dalam tinjauan ini secara otomatis mengecualikan variasi serangan pada sistem infrastruktur kritis yang berbasis pada protokol industri khusus. Dengan menyadari keterbatasan tersebut, tahap akhir metodologi ini adalah sintesis argumentatif yang bertujuan mengevaluasi sejauh mana hibridisasi antara integrasi Big Data dan pembelajaran mesin heuristik dapat menutupi kelemahan-kelemahan sistem deteksi yang ada saat ini.

HASIL DAN PEMBAHASAN

Hasil analisis terhadap berbagai kasus serangan menunjukkan bahwa keberhasilan infiltrasi malware sering kali bukan disebabkan oleh kecanggihan kode semata, melainkan oleh eksploitasi terhadap titik lemah interaksi manusia. Investigasi pada malware njRAT (Rizky et al., 2016) menegaskan bahwa rekayasa sosial tetap menjadi vektor utama yang melampaui proteksi teknis manapun. Namun, temuan ini harus dikontraskan dengan pergeseran metode serangan pada infrastruktur yang lebih kritikal: jika pada level personal social engineering mendominasi, pada sektor perbankan dan cloud, serangan seperti Ryuk lebih mengandalkan otomatisasi eksploitasi protokol dan penyalahgunaan panggilan API (API Calls) yang sah (Wijanarko et al., 2023). Fenomena ini memicu perdebatan metodologis: apakah kita harus terus memperkuat dinding api (firewall) atau mulai beralih sepenuhnya pada pemantauan perilaku akses data yang dianggap “normal” namun destruktif.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Efektivitas Kecerdasan Buatan (AI) dalam deteksi malware memberikan data yang menjanjikan sekaligus mencemaskan. Implementasi Decision Tree dengan Information Gain terbukti mampu meningkatkan akurasi klasifikasi file eksekusi pada Windows hingga level yang sangat presisi (Aditya Pratama & Murdiansyah, 2025). Namun, optimisme terhadap model tunggal ini perlu dipertentangkan dengan efisiensi Ensemble Learning pada platform Android (Azwar et al., 2025), yang menunjukkan bahwa penggabungan beberapa model justru lebih stabil dalam menghadapi trojan perbankan yang dinamis. Kritik utama yang muncul dari perbandingan ini adalah bahwa akurasi tinggi di laboratorium sering kali bersifat semu; sistem ini kerap gagal saat berhadapan dengan adversarial attacks (Andi Novianto, 2025) yang sengaja memanipulasi fitur malware untuk mengelabui logika pembelajaran mesin. Hal ini memaksa kita untuk mengakui keterbatasan sistem cerdas saat ini: AI hanya sekuat data pelatihnya, dan penyerang kini mulai belajar cara "meracuni" data tersebut.

Dari sisi respons insiden, temuan investigasi forensik mengungkapkan realitas durasi serangan yang sangat agresif. Fakta bahwa Ryuk mampu mengenkripsi seluruh aset digital dalam waktu 10 menit (Kusuma, 2023) meruntuhkan relevansi metode investigasi tradisional yang bersifat pasca-kejadian. Sebagai pembanding, penggunaan alat Hunchly (Na'im et al., 2023) dalam investigasi media sosial menunjukkan bahwa kecepatan pengumpulan bukti secara live adalah variabel penentu dalam menghentikan penyebaran informasi berbahaya. Pertentangan di sini sangat jelas: investigasi manual sudah tidak relevan; masa depan keamanan siber bergantung pada kemampuan alat forensik untuk melakukan isolasi otomatis dalam milidetik, bukan sekadar pelaporan administratif setelah sistem lumpuh.

Terakhir, strategi mitigasi melalui optimalisasi perangkat lunak seperti ClamAV (Syahrial Athoriq Nadzar & Servanda, 2024) sering kali dipandang sebagai solusi ekonomis bagi sistem Windows. Akan tetapi, strategi ini bersifat sangat terbatas jika tidak dibarengi dengan skema recovery yang teruji. Simulasi serangan pada database Bank Syariah Indonesia (Wijanarko et al., 2023) membuktikan bahwa cadangan data (backup) adalah pertahanan terakhir yang mutlak, namun efektivitasnya tetap bergantung pada integrasi Cyber Threat Intelligence yang proaktif (Kristian et al., 2025). Jurnal ini menyimpulkan bahwa mitigasi tidak boleh hanya berfokus pada pencegahan infeksi, melainkan harus mencakup ketahanan sistem untuk tetap beroperasi meskipun dalam kondisi terinfeksi. Keterbatasan pembahasan pada bab ini terletak pada belum diujinya model pertahanan hibrida ini pada jaringan nirkabel berskala luas yang memiliki latensi tinggi.

KESIMPULAN

Evolusi virus dan malware yang dibedah dalam studi ini membawa kita pada satu tesis utama: bahwa kedaulatan keamanan siber tidak lagi ditentukan oleh seberapa tebal "dinding" proteksi yang dibangun, melainkan oleh seberapa adaptif sistem dalam mengelola anomali. Pertanyaan awal mengenai efektivitas edukasi dan teknologi terjawab melalui realitas yang kontras; meskipun kesadaran pengguna di lingkup mahasiswa meningkat (Wahyu Hidayat M et al., 2023), hal tersebut menjadi tidak relevan ketika berhadapan dengan malware yang mengeksploitasi fungsi sistemik seperti API Calls yang sah (Hartinah et al., 2023). Kesimpulan ini menegaskan bahwa strategi penanggulangan harus berhenti memperlakukan malware sebagai objek statis dan mulai memandangnya sebagai entitas intelijen yang mampu melakukan kamuflase terhadap model pembelajaran mesin melalui serangan adversarial (Andi Novianto, 2025).

Integrasi Machine Learning dan Big Data memang menawarkan lompatan akurasi yang signifikan, namun penelitian ini menyimpulkan bahwa teknologi tersebut bukanlah peluru perak (silver bullet). Ada ketergantungan kritis pada kualitas data latih dan integritas infrastruktur cloud yang justru sering menjadi titik lemah baru dalam investigasi forensik (Kusuma, 2023). Oleh karena itu, hibridisasi antara metode deteksi proaktif berbasis perilaku dan kesiapan mitigasi pasca-infeksi (seperti simulasi pada database perbankan) adalah satu-satunya jalan rasional dalam menghadapi ketidakpastian ancaman di masa depan. Keterbatasan jujur dari kajian ini adalah fokusnya yang masih didominasi oleh ekosistem Windows dan Android, sehingga diperlukan penelitian lebih lanjut yang mengeksplorasi ancaman pada arsitektur sistem tertutup dan perangkat IoT yang memiliki sumber daya komputasi terbatas. Akhirnya, keamanan siber adalah proses berkelanjutan yang menuntut sinergi antara ketajaman algoritma dan skeptisisme manusia yang teredukasi.

REFERENSI

Adenansi, R., & A. Novarina, L. (2017). Malware Dynamic. *Jurnal of Education and Information Communication Technology*, *1*, 37–43.

Aditya Pratama, R., & Murdiansyah, D. T. (2025). Sistem Deteksi Malware Menggunakan Information Gain dan Decision Tree. *CESS (Journal of Computer Engineering, System and Science)*, *10*(2), 656–665. https://doi.org/10.24114/cess.v10i2.67170

Andi Novianto. (2025). Deteksi Malware Adversarial pada Jaringan IoT: Tinjauan Sistematis Model AI dan Strategi Serangan. *DutaCom*, *18*(2). https://doi.org/10.47701/dutacom.v18i2.5128

Aura Jelita, N. B., & Siregar, H. (2025). Systematic Literature Review: Evolusi Ancaman Siber Dan Metode Deteksi

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Malware Di Sistem Operasi Android (2020–2025). *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(1), 227–235. https://doi.org/10.62712/juktisi.v4i1.395

Azwar, M., Widyawati, L., Azhar, R., Kartarina, K., Tanwir, T., & Anas, A. S. (2025). Deteksi Malware pada Perangkat Android Menggunakan Ensemble Learning. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *7*(3), 408–419. https://doi.org/10.35746/jtim.v7i3.573

Hartinah, Wahyudi Paundu, A., & Ahmad Ilham, A. (2023). *Deteksi Malware Ransomware berdasarkan Panggilan API dengan Metode Ekstraksi Fitur N-gram dan TF-IDF*.

Karunia, W. A., Zahra, A. F., & Amrozi, Y. (2025). Evaluasi Ancaman Baru Dalam Keamanan Informasi: Systematic Literature Review Tentang Kerentanan Cyber Security Pasca-Pandemi. *Cyber Security Dan Forensik Digital*, *8*(1), 10–16. https://doi.org/10.14421/csecurity.2025.8.1.4889

Kristian, A., Skavinsky Teddy, R., Meylani, V. P., & Kesuma, D. P. (2025). Strategi Mitigasi Ancaman Siber di Era Teknologi Berkembang: Systematic Literature Review. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *8*(3).

Kusuma, R. S. (2023). Forensik Serangan Ransomware Ryuk pada Jaringan Cloud. *MULTINETICS*, *9*(2), 99–107. https://doi.org/10.32722/multinetics.v9i2.5234

murwodo, sudeng. (2023). Mengenal lebih dalam tentang virus virus komputer dan perilakunya. *Jurnal Ilmiah Infokam*. https://doi.org/10.53845/infokam.v19i1.344

Na'im, M., Jum'ah, A., Wijaya, H., & Ismail, R. R. (2023). *Implementasi Model Digital Forensik Proses (DFD) Untuk Sosial Media Investigation Dengan Tools Hunchly* (Vol. 6, Issue 2). https://doi.org/10.14421/csecurity.2023.6.2.4265

Rizky, D. septani, Widiyasono, N., & Mubarok, H. (2016). Investigasi Serangan Malware Njrat Pada PC. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2).

Sumarno, S. (2023). Analisis Cara Kerja Sistem Deteksi Infeksi Worm Pada Komputer. *METIK JURNAL*, *7*(2), 93–100. https://doi.org/10.47002/metik.v7i2.636

Syahrial Athoriq Nadzar, M., & Servanda, Y. (2024). Optimalisasi Keamanan Windows: Implementasi Clamav Tools Untuk Proteksi Antivirus. *Jurnal Sains Dan Teknologi (JSIT)*, *4*(2), 168–174. https://doi.org/10.47233/jsit.v4i2.1829

Tiana, D., Supriyadi, O., Wahyudi, B., Rimbawa, D., Program, P., Rekayasa, S., Siber, P., & Pertahanan, U. (2025). *Studi Pustaka: Optimalisasi Deteksi Malware melalui Integrasi Pembelajaran Mesin Heuristik dan Big Data untuk Keamanan Siber*. *14*(1), 2715–7849. https://doi.org/10.34010/komputa.v14i1

Wahyu Hidayat M, Muhammad Arqam Syahputra, Muh. Fadlan Amrullah, Lisdayanti Susanto, & Andi Shelma Putri. (2023). Analisis Upaya Meningkatkan Keamanan Komputer Terhadap Ancaman di Lingkup Mahasiswa. *Indonesian Technology and Education Journal*, *1*(1), 29–36. https://doi.org/10.61255/itej.v1i1.44

Wijanarko, R. P., Moch Rezeki Setiawan, Siti Mukaromah, & Abdul Rezha Efrat Najaf. (2023). ANALISIS DAN SIMULASI SERANGAN RANSOMWARE TERHADAP DATABASE BANK SYARIAH INDONESIA. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), 106–115. https://doi.org/10.33005/sitasi.v3i1.436