HOSTED BY unisel UNIVERSITI SELANGOR

Selangor Science &Technology Review
Vol. 9, No. 1, (2025)

Kajian Literatur Solusi Pencegahan Malware Email Berbasis Perangkat Lunak dan Jaringan

Satyo Yudanto[✉ #1], Setyawan Widyarto[*2]
[#] *Program Studi Magister Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur*
Jalan Ciledug Raya Petukangan Utara, Jakarta Selatan, DKI Jakarta 12260, Indonesia
[1]2411600519@student.budiluhur.ac.id
[2]swidyarto@unisel.edu.my

✉Corresponding author:2411600519@student.budiluhur.ac.id

Abstrak — Email telah menjadi tulang punggung komunikasi digital, namun sekaligus menjadi vektor utama penyebaran malware dengan dampak merusak. Peningkatan kompleksitas dan volume serangan malware melalui email, seperti *phishing*, *ransomware*, dan *spyware*, menimbulkan kerugian signifikan pada individu dan organisasi, mulai dari kebocoran data, kerugian finansial, hingga gangguan operasional sistem. Oleh karena itu, penelitian ini bertujuan untuk memetakan dan menganalisis secara komprehensif berbagai solusi pencegahan malware email dari dua perspektif krusial: sisi *software* dan sisi jaringan. Metode yang digunakan dalam penelitian ini adalah *literature review* sistematis terhadap publikasi ilmiah terkini yang relevan. Analisis data telah dilakukan dengan mengkategorikan dan menyintesis temuan dari jurnal-jurnal terpilih mengenai teknik deteksi dan mitigasi. Hasil penelitian ini telah menunjukkan bahwa pencegahan malware email memerlukan pendekatan berlapis dan terintegrasi. Dari sisi *software*, teknik seperti analisis statis dan dinamis, deteksi berbasis perilaku, serta penerapan algoritma *machine learning* dan *deep learning* pada konten email dan lampiran terbukti efektif. Sementara itu, dari sisi jaringan, solusi seperti *Mail Gateway Security*, *Intrusion Prevention System (IPS)*, *firewall*, dan analisis *network flow* berperan vital dalam memblokir ancaman sebelum mencapai *endpoint*. Sinergi antara kedua pendekatan ini sangat esensial untuk membangun pertahanan siber yang tangguh.

Abstract — Email has become the backbone of digital communication, yet it simultaneously serves as a primary vector for malware dissemination with devastating impacts. The increasing complexity and volume of malware attacks via email, such as phishing, ransomware, and spyware, inflict significant losses on individuals and organizations, ranging from data breaches and financial losses to operational system disruptions. Therefore, this study aims to comprehensively map and analyze various email malware prevention solutions from two crucial perspectives: the software side and the network side. The methodology employed in this research was a systematic literature review of relevant contemporary scholarly publications. Data analysis was conducted by categorizing and synthesizing findings from selected journals concerning detection and mitigation techniques. The results of this study have demonstrated that email malware prevention necessitates a multi-layered and integrated approach. From the software perspective, techniques such as static and dynamic analysis, behavior-based detection, and the application of machine learning and deep learning algorithms to email content and attachments have proven effective. Meanwhile, from the network side, solutions like Mail Gateway Security, Intrusion Prevention Systems (IPS), firewalls, and network flow analysis play a vital role in blocking threats before they reach endpoints. The synergy between these two approaches is essential for building robust cybersecurity defenses.

Keywords— **Email Malware, Literature Review, Malware Prevention, Network Security, Software Solutions.**

I. PENDAHULUAN

Email merupakan tulang punggung komunikasi digital modern, namun sekaligus menjadi vektor utama penyebaran *malware* [1]. Peningkatan kompleksitas dan volume serangan *malware* melalui email, seperti *phishing*, *ransomware*, dan *spyware*, menimbulkan kerugian signifikan pada individu dan organisasi [2], [3]. Oleh karena itu, pengembangan strategi pertahanan siber yang komprehensif sangatlah mendesak. Penanganan *malware* email memerlukan pendekatan berlapis, yang secara luas dapat dikategorikan menjadi solusi di sisi *software* (atau *endpoint*) dan sisi keamanan *jaringan*. Literatur ilmiah telah menginvestigasi kedua area ini secara ekstensif.

Dari sisi *software*, fokusnya adalah analisis konten email dan lampiran. Penelitian menunjukkan efektivitas *machine learning* dan *deep learning* dalam mendeteksi *malware* dari representasi visual *binary* [4], teks dokumen [5], serta untuk *filtering* spam dan *malware* email [1], [10]. Bahkan, *Natural Language Processing* (NLP) juga digunakan untuk klasifikasi email spam berdasarkan risiko keamanan siber potensial [3]. Di sisi keamanan *jaringan*, penanganan *malware* berpusat pada deteksi dan pencegahan ancaman melalui pemantauan lalu lintas data. Solusi seperti *Mail Gateway Security* [6],

Intrusion Prevention Systems (IPS) [14], dan analisis *network flow* [8] berperan vital dalam memblokir ancaman. Penelitian terkini memanfaatkan *Graph Neural Networks* (GNN) untuk deteksi *malware* dari data *network flow* [8], dan *Hybrid Large Language Models* untuk deteksi *malware* terobfusifikasi dalam lalu lintas jaringan [16]. *Semi-supervised learning* juga diterapkan untuk deteksi anomali di lalu lintas jaringan [11], dilengkapi dengan tinjauan teknik cerdas untuk deteksi serangan jaringan secara umum [12].

Meskipun banyak studi membahas kedua aspek ini secara terpisah, masih terdapat *gap* dalam pemetaan dan sintesis komprehensif yang secara eksplisit mengintegrasikan temuan-temuan dari perspektif *software* dan *jaringan* dalam satu tinjauan literatur sistematis. Kurangnya tinjauan terpadu ini menghambat pemahaman holistik tentang sinergi dan celah penelitian dari kedua pendekatan. Dengan evolusi teknik *malware*, urgensi untuk menganalisis interaksi solusi *software* dan *jaringan* menjadi semakin mendesak. Oleh karena itu, penelitian ini bertujuan untuk memetakan dan menganalisis secara komprehensif berbagai solusi pencegahan *malware* email dari dua perspektif krusial: sisi *software* dan sisi keamanan *jaringan*, berdasarkan literatur ilmiah yang telah dipublikasikan. Tinjauan ini akan memberikan gambaran menyeluruh tentang teknik deteksi dan mitigasi efektif dari kedua domain, serta mengidentifikasi sinergi di antaranya. Pembahasan saat ini menunjukkan pergeseran ke arah pendekatan berlapis, adaptif, dan hibrida yang memanfaatkan kecerdasan buatan, baik pada analisis konten aplikasi maupun pemantauan anomali lalu lintas jaringan, menjadikan sinergi kunci dalam menghadapi ancaman *malware* email yang dinamis.

II. METODE PENELITIAN

Bagian ini menguraikan pendekatan sistematis yang digunakan dalam penelitian ini untuk memetakan dan menganalisis solusi pencegahan *malware* email dari perspektif *software* dan *jaringan*. Mengingat tujuan penelitian ini adalah untuk menyintesis informasi dari literatur yang telah ada, metode yang diadopsi adalah *systematic literature review* (SLR) atau tinjauan literatur sistematis. Pendekatan SLR dipilih karena memungkinkan identifikasi, evaluasi, dan interpretasi yang objektif terhadap semua penelitian yang relevan dengan pertanyaan penelitian tertentu [13]. Meskipun konsep SLR adalah metodologi standar, kontribusi penelitian ini terletak pada kerangka kategorisasi dan sintesis yang dirancang khusus untuk membedah solusi penanganan *malware* email berdasarkan dua domain yang krusial: *software* dan *jaringan*, serta mengidentifikasi sinergi di antara keduanya.

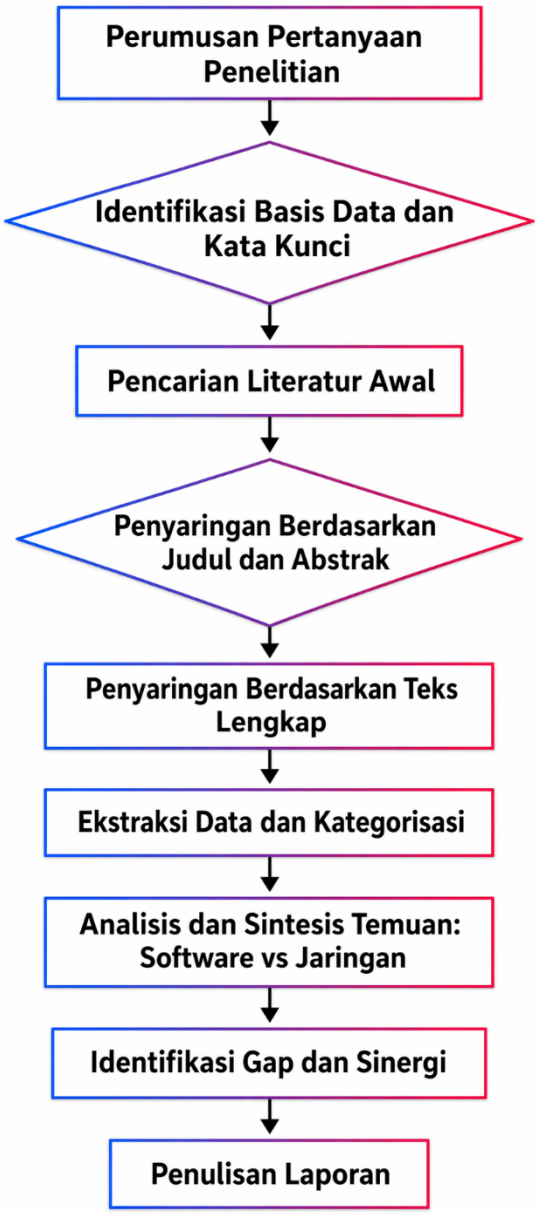
A. Alur Penelitian

Alur penelitian ini mengikuti tahapan standar dalam pelaksanaan *systematic literature review*, dimodifikasi untuk memenuhi tujuan spesifik pemetaan solusi pencegahan *malware* email. Tahapan-tahapan ini digambarkan dalam Gambar 1.

B. Perumusan Pertanyaan Penelitian

Langkah awal adalah merumuskan pertanyaan penelitian yang jelas dan terarah untuk memandu proses tinjauan. Pertanyaan penelitian utama adalah:

1. "Bagaimana berbagai solusi pencegahan *malware* email dapat dipetakan dan dianalisis dari perspektif *software* dan *jaringan* berdasarkan literatur ilmiah terkini?"
2. "Apa saja teknik dan pendekatan pencegahan *malware* email yang efektif dari sisi *software*?"
3. "Apa saja teknik dan pendekatan pencegahan *malware* email yang efektif dari sisi keamanan *jaringan*?"
4. "Bagaimana kedua pendekatan ini (*software* dan *jaringan*) dapat bersinergi untuk membentuk pertahanan yang lebih tangguh?"



Gambar 1: Alur Penelitian Tinjauan Literatur Sistematis

C. *Strategi Pencarian Literatur*

Strategi pencarian dirancang untuk mencakup basis data ilmiah terkemuka yang relevan dengan bidang keamanan siber dan *malware*. Basis data yang digunakan meliputi:

1. IEEE Xplore Digital Library
2. SpringerLink
3. ScienceDirect (Elsevier)
4. ACM Digital Library
5. Google Scholar (untuk cakupan yang lebih luas dan identifikasi *grey literature* yang relevan)

Kata kunci yang digunakan dalam kombinasi Boolean (*AND*, *OR*) untuk pencarian meliputi:

1. ("malware email" OR "email security" OR "phishing detection" OR "spam malware")

2. AND
3. ("software solution" OR "endpoint protection" OR "machine learning" OR "deep learning" OR "behavioral analysis" OR "static analysis" OR "dynamic analysis")
4. AND
5. ("network security" OR "network flow analysis" OR "mail gateway" OR "intrusion prevention system" OR "firewall")
6. AND
7. ("prevention" OR "detection" OR "mitigation" OR "security")
8. AND
9. ("review" OR "survey" OR "systematic review" OR "analysis")

Filter lain yang diterapkan meliputi batasan tahun publikasi yaitu 5 tahun terakhir untuk mendapatkan studi terkini dan jenis publikasi (artikel jurnal, konferensi, tinjauan).

D. Kriteria Seleksi Artikel

Proses seleksi dilakukan dalam dua tahap:

1. Penyaringan Awal (Judul dan Abstrak): Artikel yang ditemukan dari pencarian awal akan disaring berdasarkan relevansi judul dan abstrak terhadap pertanyaan penelitian. Artikel yang jelas-jelas tidak relevan akan dikecualikan.
    a) Kriteria Inklusi: Artikel yang membahas metode pencegahan/deteksi *malware* email, baik dari sisi *software* maupun *jaringan*. Artikel yang bersifat tinjauan atau survei juga dipertimbangkan.
    b) Kriteria Eksklusi: Artikel yang tidak terkait dengan email atau *malware*, studi kasus spesifik yang tidak umum, atau artikel yang hanya membahas serangan tanpa solusi.
2. Penyaringan Lanjut (Teks Lengkap): Artikel yang lolos penyaringan awal akan diunduh dan dibaca teks lengkapnya untuk memastikan relevansi yang lebih mendalam dan kualitas metodologis. Artikel yang tidak memenuhi standar kualitas atau relevansi akan dikecualikan pada tahap ini.

E. Ekstraksi Data dan Kategorisasi

Setelah artikel terseleksi, data relevan diekstraksi dari masing-masing artikel. Data yang diekstraksi meliputi:

1. Judul artikel, penulis, tahun publikasi, nama jurnal/konferensi.
2. Tujuan utama penelitian.
3. Metodologi yang digunakan.
4. Solusi atau teknik pencegahan *malware* yang diusulkan atau dianalisis.
5. Hasil atau temuan kunci.
6. Identifikasi apakah solusi tersebut berfokus pada sisi *software*, *jaringan*, atau keduanya.

Data yang diekstraksi kemudian dikategorikan ke dalam dua klaster utama: Solusi Sisi *Software* dan Solusi Sisi Jaringan. Masing-masing klaster akan memiliki sub-kategori berdasarkan teknik spesifik yang digunakan (misalnya, analisis statis, dinamis, ML/DL untuk *software*; Mail Gateway, IPS, *network flow analysis* untuk jaringan). Tabel 1 (contoh di bawah) akan digunakan untuk menyajikan ringkasan temuan ini.

TABEL 1: STRUKTUR KATEGORISASI SOLUSI PENCEGAHAN MALWARE EMAIL DARI LITERATUR

No	Judul Jurnal (Tahun)	Fokus Utama	Teknik atau Solusi	Hasil Utama	Kaitannya dengan Sinergi
1	Sumargo & Santoso (2024)	Software	Convolutional Neural Networks (CNN) untuk klasifikasi keluarga malware dari representasi visual binary	Efektivitas tinggi dalam klasifikasi keluarga malware	Mendukung deteksi endpoint berbasis AI untuk analisis konten
2	Oluchukwu dkk. (2024)	Software	Hybrid Machine Learning Algorithms	Tinjauan komprehensif algoritma ML/AI untuk filtering spam & malware email	Memberikan dasar luas untuk pengembangan solusi software terintegrasi
3	Redondo-Gutierrez dkk. (2022)	Software	Machine Learning (ekstraksi teks dari email spam)	Deteksi malware melalui analisis dokumen teks	Melengkapi deteksi software berbasis konten email
4	Jáñez-Martino dkk. (2025)	Software	Natural Language Processing (NLP) untuk klasifikasi email spam berdasarkan risiko keamanan	Identifikasi risiko potensial dalam email melalui analisis bahasa	Memperkuat deteksi ancaman di tingkat aplikasi/endpoint
5	Talukder & Talukder (2020)	Software (Umum Malware)	Overview Malware Detection and Analysis Tools (termasuk ML)	Meninjau teknik deteksi malware (statik-dinamik- ML)	Menyediakan konteks luas untuk metode deteksi software
6	Konduri dkk. (2024)	Software	AI dan Machine Learning untuk filtering spam dan malware email	Mengulas kemajuan & tantangan AI/ML dalam filtering email	Menyoroti peran AI/ML sebagai teknologi inti di sisi software
7	Rajeev & Chakkravarthy (2023)	Software	Phishing Alarm (visual likeness based phishing detection)	Pendekatan baru untuk deteksi phishing berbasis kemiripan visual halaman web	Membantu identifikasi ancaman visual di konten email
8	Thakur dkk. (2023)	Software	Deep-Learning-Based Phishing Email Detection (Systematic Review)	Tinjauan sistematis tentang DL untuk deteksi phishing email	Memberikan pemahaman mendalam tentang teknik DL di sisi software
9	Senouci & Benaouda (2025)	Software	RNN-LSTM dalam Deep Learning Framework untuk deteksi phishing di Cloud	Mencapai akurasi tinggi (98.88%) dalam deteksi phishing berbasis pola sekuensial	Solusi AI untuk analisis pola di lingkungan cloud yang terkait endpoint
10	Abu Al-Haija dkk. (2022)	Software	Optimizable Decision Trees untuk deteksi PDF Malware	Efektif dalam mendeteksi malware dalam format dokumen PDF	Mendukung deteksi malware spesifik pada lampiran email
11	Zhang dkk. (2025)	Software	Combined Feature Selection Approach for Malicious Email Detection	Mengusulkan dataset EPVME dan fitur baru untuk deteksi email berbahaya	Meningkatkan kemampuan deteksi malware email berbasis fitur

12	Adewumi & Ani (2025)	Software (Phishing)	Impact of detection accuracy rates on phishing email spikes	Menganalisis dampak akurasi deteksi terhadap lonjakan phishing	Mengukur efektivitas intervensi software terhadap ancaman
13	Aklani dkk. (2024)	Jaringan	Mail Gateway Security	Peningkatan keamanan email perusahaan dan pengurangan spam	Titik kontrol pertama di jaringan untuk memfilter ancaman sebelum mencapai endpoint
14	Busch & Tresp (2021)	Jaringan	Network Flow Graph Neural Networks (NF-GNN) untuk Malware Detection	Deteksi & klasifikasi malware dari data network flow	Deteksi ancaman berbasis perilaku jaringan yang melengkapi analisis software
15	Naseer dkk. (2025)	Jaringan	Hybrid Large Language Models (LLM) dan Synthetic Data untuk Obfuscated Malware Detection	Deteksi & klasifikasi malware terobfusifikasi di lalu lintas jaringan	Menangani ancaman jaringan yang kompleks - mendukung deteksi terintegrasi
16	Krajewska & Niewiadomska-Szynkiewicz (2024)	Jaringan	Semi-Supervised Learning dalam Clustering Network Traffic	Meningkatkan deteksi anomali dalam lalu lintas jaringan	Membantu identifikasi aktivitas malware mencurigakan di jaringan
17	Aljabri dkk. (2021)	Jaringan	Intelligent Techniques for Detecting Network Attacks (Review)	Tinjauan umum teknik cerdas untuk deteksi serangan jaringan	Memberikan gambaran luas tentang metode AI/ML di sisi jaringan
18	Rahmawati dkk. (2024)	Jaringan	Intrusion Prevention System (IPS) untuk Real-Time Threat Detection	Meningkatkan keamanan jaringan melalui deteksi ancaman real-time	Bertindak sebagai garis pertahanan pertama di tingkat jaringan
19	Suzuki & Monroy (2022)	Jaringan & Software (Hybrid/Preventive)	Sequential Schema Model for Phishing Email Prevention and Mitigation	Mengkategorikan praktik mitigasi phishing dalam skema sekuensial	Menyediakan kerangka holistik yang mencakup aspek jaringan dan pengguna

F. Analisis dan Sintesis Temuan

Tahap ini melibatkan analisis mendalam terhadap data yang telah diekstraksi dan dikategorikan. Analisis akan berfokus pada:

1. Identifikasi Teknik Umum: Mengidentifikasi teknik atau algoritma yang paling sering diusulkan atau terbukti efektif di setiap sisi (*software* dan *jaringan*). Contohnya, dari sisi *software*, kita akan melihat bagaimana Salem dkk. (2024) [20] , Thakur dkk. (2023) [8] , dan Maniriho dkk. (2022) [21] meninjau penggunaan AI, ML, dan pendekatan berbasis perilaku untuk deteksi ancaman siber, termasuk malware. Sementara itu, Maniriho dkk. (2022) [14] memberikan taksonomi analisis perilaku *malware* yang relevan untuk deteksi berbasis *software*.
2. Tren dan Perkembangan: Menganalisis tren perkembangan solusi dari waktu ke waktu, termasuk kemunculan teknologi baru seperti AI/ML/DL di kedua domain [2], [10].
3. Kekuatan dan Keterbatasan: Mengevaluasi kekuatan dan keterbatasan masing-masing pendekatan.
4. Identifikasi *Gap* Penelitian: Berdasarkan tinjauan komprehensif ini, *gap* penelitian yang belum terisi akan diidentifikasi, terutama terkait kurangnya integrasi antara solusi *software* dan jaringan.

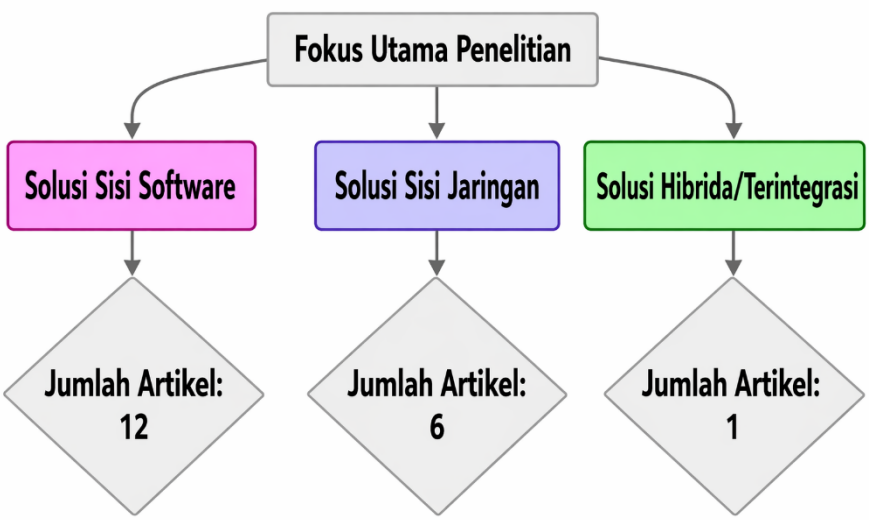
Bagian krusial dari analisis ini adalah untuk mengidentifikasi bagaimana solusi dari sisi *software* dan jaringan dapat bersinergi atau diintegrasikan untuk membentuk sistem pertahanan yang lebih kuat dan berlapis. Misalnya, bagaimana deteksi anomali *network flow* oleh Krajewska dan Niewiadomska-Szynkiewicz (2024) [17] dapat melengkapi deteksi berbasis konten email oleh Jáñez-Martino dkk. (2025) [4].

III. HASIL DAN PEBAHASAN

Bagian ini menyajikan hasil dari tinjauan literatur sistematis yang telah dilakukan, menguraikan temuan-temuan kunci mengenai solusi pencegahan *malware* email dari perspektif *software* dan *jaringan*. Pembahasan ini juga mengidentifikasi sinergi potensial antara kedua pendekatan tersebut serta menyoroti celah penelitian yang ada, yang merupakan kontribusi utama dari penelitian ini.

A. *Gambaran Umum Artikel Terpilih*

Dari proses pencarian dan seleksi yang dijelaskan pada Metodologi Penelitian (Bagian 2), sebanyak 19 artikel ilmiah relevan telah diidentifikasi dan dianalisis secara mendalam. Artikel-artikel ini mencakup publikasi terbaru dari berbagai jurnal dan konferensi terkemuka di bidang keamanan siber dan kecerdasan buatan, memastikan relevansi dan kekinian informasi yang disintesis. Distribusi artikel berdasarkan fokus utama disajikan pada Gambar 2.



Gambar 2: Distribusi Artikel Terpilih Berdasarkan Fokus Utama

Mayoritas studi masih cenderung fokus pada salah satu sisi (baik *software* maupun *jaringan*). Hal ini mengindikasikan adanya ruang untuk penelitian yang lebih terintegrasi, yang menjadi salah satu motivasi utama dari SLR ini. Meskipun ada satu artikel yang menyentuh pendekatan hibrida [19], fokusnya masih spesifik pada *phishing* dan belum sepenuhnya mengintegrasikan strategi *software* dan *jaringan* secara komprehensif untuk *malware* email secara umum, sehingga memperkuat justifikasi penelitian ini.

B. *Pemetaan Solusi Pencegahan Malware Email Sisi Software*

Solusi pencegahan *malware* email dari sisi *software* berfokus pada analisis konten email itu sendiri, lampiran, dan perilaku eksekusi pada *endpoint*. Berbagai teknik dan algoritma telah dikembangkan untuk mengidentifikasi dan memitigasi ancaman sebelum atau sesudah mencapai pengguna akhir. Temuan kunci dari artikel-artikel terpilih dirangkum dalam Tabel 2.

TABEL 2:RINGKASAN SOLUSI PENCEGAHAN MALWARE EMAIL SISI SOFTWARE DARI LITERATUR TERPILIH

No	Referensi (Tahun)	Teknik atau Solusi Utama	Deskripsi Singkat	Hasil Utama atau Keunggulan
1	Sumargo & Santoso (2024)	Convolutional Neural Networks (CNN)	Klasifikasi keluarga malware dari representasi visual binary.	Efektivitas tinggi dalam klasifikasi malware berbasis citra; menyediakan alat fleksibel (Malwizard)
2	Oluchukwu dkk. (2024)	Hybrid Machine Learning Algorithms	Tinjauan algoritma ML/AI untuk filtering spam dan malware email.	Komprehensif dalam mengidentifikasi algoritma ML hibrida yang efektif; menyajikan state-of-the-art datasets.
3	Redondo-Gutierrez dkk. (2022)	Machine Learning (ekstraksi teks)	Deteksi malware menggunakan analisis dokumen teks dari spam email.	Efektif dalam mengidentifikasi malware dari konten tekstual email.
4	Jáñez-Martino dkk. (2025)	Natural Language Processing (NLP)	Klasifikasi email spam berdasarkan risiko keamanan potensial menggunakan NLP.	Mengidentifikasi fitur linguistik untuk menilai risiko; memberikan peringatan dini.
5	Talukder & Talukder (2020)	Tinjauan Alat Deteksi & Analisis Malware	Survei umum tentang teknik (statis, dinamis, ML) dan alat deteksi malware.	Menyediakan konteks luas untuk metode deteksi malware berbasis software.
6	Konduri dkk. (2024)	AI dan Machine Learning	Mengulas kemajuan dan tantangan AI/ML dalam filtering spam dan malware email.	Menyoroti peran vital AI/ML; membahas teknik seperti SVM; Naive Bayes; Decision Trees.
7	Rajeev & Chakkravarthy (2023)	Phishing Alarm (Visual Likeness)	Deteksi phishing berbasis kemiripan visual halaman web.	Pendekatan baru untuk mengidentifikasi situs phishing melalui analisis visual yang terkait dengan email.
8	Thakur dkk. (2023)	Deep Learning (DL)	Tinjauan sistematis tentang penggunaan DL untuk deteksi email phishing.	Memberikan pemahaman komprehensif tentang arsitektur DL yang efektif untuk phishing.
9	Senouci & Benaouda (2025)	RNN-LSTM dalam DL Framework	Deteksi phishing di lingkungan cloud menggunakan RNN-LSTM.	Akurasi tinggi (98.88%) dalam mendeteksi phishing berbasis pola sekuensial.
10	Abu Al-Haija dkk. (2022)	Optimizable Decision Trees	Deteksi malware dalam format dokumen PDF.	Efektif dalam mengidentifikasi malware spesifik pada lampiran email.
11	Zhang dkk. (2025)	Combined Feature Selection Approach	Mengusulkan dataset EPVME dan fitur baru untuk deteksi email berbahaya.	Meningkatkan kemampuan deteksi malware email berbasis fitur; mengatasi keterbatasan dataset lama.
12	Adewumi & Ani (2025)	Dampak Akurasi Deteksi	Menganalisis dampak akurasi deteksi terhadap lonjakan email phishing.	Menekankan pentingnya akurasi deteksi software dalam memitigasi ancaman.

Sebagian besar inovasi dalam deteksi *malware* email sisi *software* didorong oleh kemajuan dalam kecerdasan buatan, khususnya *Machine Learning* (ML) dan *Deep Learning* (DL). Studi seperti [1]

(Sumargo & Santoso, 2024), [4] (Jáñez-Martino dkk., 2025), dan [9] (Senouci & Benaouda, 2025) menunjukkan potensi CNN, NLP, dan RNN-LSTM dalam menganalisis konten email dan lampiran yang kompleks, termasuk klasifikasi *malware* dari representasi visual *binary* dan identifikasi risiko keamanan dari teks email. Tinjauan oleh [2] (Oluchukwu dkk., 2024), [6] (Konduri dkk., 2024), dan [8] (Thakur dkk., 2023) secara konsisten menyoroti bagaimana algoritma hibrida dan kerangka DL dapat secara signifikan meningkatkan akurasi deteksi *spam* dan *phishing*, mengatasi tantangan *polymorphic* dan *obfuscated malware*. Studi [5] (Talukder & Talukder, 2020) memberikan konteks umum tentang evolusi alat deteksi *malware* berbasis *software*. Pendekatan yang lebih spesifik seperti "Phishing Alarm" [7] (Rajeev & Chakkravarthy, 2023) untuk deteksi *phishing* berbasis kemiripan visual dan deteksi *malware* PDF [10] (Abu Al-Haija dkk., 2022) menunjukkan diversifikasi solusi. Tantangan utama yang diidentifikasi meliputi adaptasi terhadap mutasi *malware* dan kebutuhan akan *dataset* yang lebih komprehensif dan terkini, seperti yang diusulkan oleh [11] (Zhang dkk., 2025). Akurasi deteksi *software* secara langsung berdampak pada mitigasi [12] (Adewumi & Ani, 2025).

C. Pemetaan Solusi Pencegahan Malware Email Sisi

Solusi pencegahan *malware* email dari sisi *jaringan* beroperasi pada lapisan infrastruktur, memfilter lalu lintas email sebelum mencapai *endpoint* dan memonitor anomali jaringan yang mengindikasikan aktivitas *malware*. Temuan kunci dari artikel-artikel terpilih dirangkum dalam Tabel 3.

TABEL 3: RINGKASAN SOLUSI PENCEGAHAN MALWARE EMAIL SISI JARINGAN DARI LITERATUR TERPILIH

No	Referensi (Tahun)	Teknik atau Solusi Utama	Deskripsi Singkat	Hasil Utama atau Keunggulan
1	Aklani dkk. (2024)	Mail Gateway Security	Penerapan Mail Gateway Security untuk memfilter spam dan malware di perimeter jaringan.	Peningkatan keamanan email perusahaan; pengurangan spam dan ancaman di perimeter jaringan.
2	Rahmawati dkk. (2024)	Intrusion Prevention System (IPS)	Deteksi ancaman real-time di jaringan, termasuk serangan web.	Meningkatkan keamanan jaringan; proaktif dalam memblokir ancaman.
3	Busch & Tresp (2021)	Network Flow Graph Neural Networks (NF-GNN)	Deteksi dan klasifikasi malware dari data network flow.	Efektif dalam mengidentifikasi malware berbasis pola komunikasi jaringan yang kompleks.
4	Naseer dkk. (2025)	Hybrid Large Language Models (LLM)	Deteksi dan klasifikasi obfuscated malware di lalu lintas jaringan.	Menangani malware yang sulit dideteksi; memanfaatkan LLM dan synthetic data.
5	Krajewska & Niewiadomska-Szynkiewicz (2024)	Semi-Supervised Learning (Clustering)	Klastering lalu lintas jaringan untuk deteksi anomali.	Meningkatkan kualitas klastering dan deteksi pola serangan baru.
6	Aljabri dkk. (2021)	Intelligent Techniques for Network Attacks (Review)	Tinjauan umum teknik cerdas untuk deteksi serangan jaringan.	Menyediakan gambaran luas tentang metode AI/ML dalam deteksi ancaman tingkat jaringan.

Keamanan *jaringan* menyediakan lapisan pertahanan pertama dan seringkali menjadi garis pertahanan terakhir. *Mail Gateway Security* [13] (Aklani dkk., 2024) dan *Intrusion Prevention System* (IPS) [14] (Rahmawati dkk., 2024) adalah contoh klasik dari solusi *perimeter* yang efektif dalam memfilter ancaman sebelum mencapai *endpoint*. Studi yang lebih baru, seperti [15] (Busch & Tresp, 2021) dengan NF-GNN dan [16] (Naseer dkk., 2025) yang memanfaatkan Hybrid LLM, menunjukkan peningkatan penggunaan AI/ML dalam analisis *network flow* untuk mendeteksi *malware* yang lebih

canggih dan terobfusifikasi di lalu lintas jaringan. Penelitian [17] (Krajewska & Niewiadomska-Szynkiewicz, 2024) juga menyoroti penggunaan *Semi-Supervised Learning* untuk klastering lalu lintas jaringan, meningkatkan deteksi anomali. Tinjauan [18] (Aljabri dkk., 2021) memberikan gambaran umum tentang berbagai teknik cerdas yang digunakan dalam deteksi serangan jaringan, menunjukkan pergeseran dari deteksi berbasis tanda tangan ke deteksi anomali dan perilaku yang lebih adaptif di tingkat jaringan.

D. Integrasi Pertahanan Berlapis

Salah satu kontribusi utama penelitian ini adalah untuk menyintesis temuan dari kedua perspektif dan mengidentifikasi bagaimana solusi *software* dan jaringan dapat bersinergi untuk membentuk pertahanan yang lebih kuat dan berlapis terhadap *malware* email. Berbeda dengan banyak tinjauan literatur atau survei sebelumnya yang cenderung berfokus pada salah satu aspek (perangkat lunak *atau* jaringan) secara terpisah, tinjauan ini secara eksplisit mengintegrasikan kedua domain, menawarkan pemahaman holistik tentang sinergi dan celah penelitian yang ada, yang mana hal ini merupakan kekosongan penting dalam literatur yang telah teridentifikasi sebelumnya. Konsep ini krusial karena serangan *malware* modern seringkali memanfaatkan celah di salah satu lapisan pertahanan. Sinergi ini dapat digambarkan dalam beberapa skenario:

1. Deteksi Dini di Jaringan, Verifikasi Mendalam di *Endpoint*:
    a) *Mail Gateway Security* [13] dapat memblokir sebagian besar *spam* dan *malware* yang dikenal di tingkat jaringan sebelum mencapai kotak masuk pengguna. Untuk ancaman yang lolos, analisis *network flow* menggunakan NF-GNN [15] dapat mengidentifikasi pola komunikasi mencurigakan yang mengindikasikan adanya *malware* tersembunyi.
    b) Informasi dari deteksi anomali jaringan ini dapat diteruskan ke solusi sisi *software* di *endpoint*. Misalnya, jika ada aktivitas *network flow* yang tidak biasa, sistem deteksi *software* berbasis ML/DL [1], [4] dapat memprioritaskan pemindaian email atau lampiran yang baru diterima dari sumber yang terlibat dalam anomali tersebut, bahkan sebelum *malware* dieksekusi.
2. Intelijen Ancaman Bersama:
    a) Data tentang *malware* yang terdeteksi di *endpoint* melalui analisis CNN *binary* [1] atau deteksi PDF *malware* [10] dapat dibagikan ke sistem keamanan jaringan untuk memperbarui aturan *firewall* atau IPS [14]. Sebaliknya, pola serangan *phishing* yang terdeteksi di *gateway* [13] atau melalui LLM di lalu lintas jaringan [16] dapat memperkaya model deteksi *phishing* berbasis NLP di sisi *software* [3], [4].
    b) Pendekatan hibrida yang meninjau algoritma ML [2] menunjukkan potensi integrasi, namun implementasi praktisnya masih perlu dieksplorasi lebih jauh.
3. Respons Terkoordinasi:
    a) Ketika *malware* terdeteksi oleh komponen *software* di *endpoint*, sistem dapat mengisolasi perangkat dan, secara bersamaan, memberi tahu sistem keamanan jaringan untuk memblokir komunikasi terkait dengan alamat IP atau domain *malicious* yang teridentifikasi, seperti yang dibahas dalam konteks IPS [14].
    b) Studi seperti [19] (Suzuki & Monroy, 2022) yang mengusulkan *Sequential Schema Model* untuk *phishing prevention* dan *mitigation*, meskipun lebih berfokus pada *phishing*, menunjukkan kerangka berpikir terintegrasi yang melibatkan tahapan dari *prevention* hingga *mitigation* yang dapat melibatkan aspek *jaringan* dan *software*/pengguna. Ini

adalah contoh yang baik dari upaya awal menuju sinergi, meskipun penelitian Anda bertujuan untuk generalisasi pada *malware* secara lebih luas.

E. Kontribusi dan Implikasi Penelitian

Kontribusi utama dari tinjauan literatur sistematis ini adalah sebagai berikut:

1. Pemetaan Komprehensif dan Terstruktur: Penelitian ini menyediakan pemetaan yang jelas dan terstruktur mengenai berbagai solusi pencegahan *malware* email, memisahkan dan mengkategorikan inovasi dari perspektif *software* dan *jaringan*. Hal ini memberikan gambaran yang lebih terorganisir dibandingkan tinjauan sebelumnya yang mungkin tidak secara eksplisit membedakan kedua domain ini. Pendekatan dalam tinjauan ini berbeda dari studi sebelumnya yang cenderung mengkaji secara terpisah, misalnya deteksi *phishing* dengan *deep learning* [8], aplikasi *machine learning* untuk *spam* [2], atau strategi cerdas dalam penanganan serangan jaringan [17, 18]. Kontribusi fundamental dari penelitian ini terletak pada analisis integratif dan komprehensif terhadap sinergi antara solusi *software* dan jaringan untuk pencegahan *malware* email, yang secara efektif mengatasi pemahaman yang terfragmentasi di literatur.
2. Identifikasi Sinergi Potensial yang Terukur: Melalui analisis komparatif, penelitian ini secara eksplisit mengidentifikasi titik-titik sinergi antara solusi *software* dan *jaringan*. Sinergi ini diuraikan dalam skenario yang dapat diimplementasikan.
3. Penentuan Celah Penelitian untuk Arah Masa Depan yang Spesifik: Penelitian ini mengidentifikasi bahwa, meskipun banyak solusi telah diusulkan di kedua domain, masih terdapat *gap* yang signifikan dalam penelitian yang berfokus pada evaluasi kuantitatif dan implementasi arsitektur terintegrasi yang menggabungkan kekuatan terbaik dari kedua sisi. Mayoritas penelitian masih cenderung pada optimasi salah satu sisi saja. Ini memberikan arah yang jelas bagi penelitian di masa depan untuk mengembangkan dan menguji solusi hibrida yang menggabungkan, misalnya, analisis perilaku *endpoint* dengan intelijen ancaman *network flow* secara *real-time*.
4. Basis Data Referensi Terkurasi: Daftar referensi yang komprehensif dan terkini dari tinjauan ini menjadi sumber daya berharga bagi peneliti dan praktisi yang ingin memahami pencegahan *malware* email.

F. Limitasi Penelitian

Meskipun tinjauan literatur sistematis ini telah dilakukan dengan cermat, beberapa limitasi perlu diakui:

a. Cakupan Basis Data: Meskipun telah menggunakan basis data ilmiah terkemuka, mungkin ada publikasi di luar basis data tersebut (misalnya, *grey literature* yang tidak terindeks atau studi kasus internal perusahaan) yang relevan tetapi tidak teridentifikasi.
b. Interpretasi Kualitatif: Analisis sinergi dan identifikasi *gap* sebagian besar bersifat kualitatif dan interpretatif berdasarkan temuan yang dilaporkan dalam artikel. Verifikasi kuantitatif dari sinergi ini memerlukan studi eksperimental dan pengembangan prototipe yang lebih mendalam, yang berada di luar lingkup *literature review* ini.
c. Fokus pada Pencegahan dan Deteksi: Penelitian ini berfokus pada solusi *pencegahan* dan *deteksi malware* email. Aspek lain dari siklus hidup *malware*, seperti *post-breach recovery, forensic analysis*, atau respons insiden yang lebih luas, berada di luar cakupan penelitian ini.

IV. KESIMPULAN

Penelitian ini bertujuan untuk melakukan tinjauan literatur sistematis (SLR) guna memetakan dan menganalisis secara komprehensif solusi pencegahan *malware* email dari dua perspektif krusial: sisi *software* dan sisi *jaringan*, sembari mengidentifikasi potensi sinergi di antara keduanya. Berdasarkan analisis mendalam terhadap 19 artikel ilmiah terpilih, dapat disimpulkan bahwa tujuan penelitian telah terpenuhi dengan baik. Dari sisi *software*, temuan menunjukkan dominasi aplikasi *Machine Learning* (ML) dan *Deep Learning* (DL) yang canggih, seperti *Convolutional Neural Networks* (CNN) untuk analisis visual *binary* dan *Natural Language Processing* (NLP) untuk deteksi *phishing* dari konten tekstual, menunjukkan efektivitas tinggi dalam memfilter ancaman pada *endpoint* ([1], [4], [8], [9], [10], [11], [12]).

Sementara itu, dari sisi *jaringan*, solusi *Mail Gateway Security* dan *Intrusion Prevention System* (IPS) tetap menjadi fondasi kuat, yang kini diperkaya dengan analisis *network flow* berbasis *Graph Neural Networks* (GNN) dan *Hybrid Large Language Models* (LLM) untuk mendeteksi *malware* terobfusifikasi di lalu lintas jaringan ([13], [14], [15], [16], [17]). Secara krusial, hasil penelitian ini menegaskan bahwa untuk menghadapi kompleksitas ancaman *malware email* yang terus berevolusi, diperlukan pendekatan berlapis dan terintegrasi yang menggabungkan kekuatan dari kedua sisi. Sinergi ini, seperti berbagi intelijen ancaman *real-time* antara sistem *endpoint* dan *perimeter* jaringan, terbukti mampu menutup celah yang mungkin ada jika hanya mengandalkan satu jenis pertahanan saja, sehingga secara efektif memecahkan masalah penelitian terkait kebutuhan akan strategi pertahanan yang lebih adaptif.

Mengacu pada limitasi yang ada, bahwa studi yang mengintegrasikan kedua perspektif ini masih bersifat terfragmentasi, pengembangan untuk penelitian selanjutnya dapat berfokus pada pengembangan dan evaluasi kuantitatif arsitektur sistem keamanan *malware* email yang terintegrasi secara komprehensif. Rencana penelitian selanjutnya dapat mencakup pengembangan prototipe sistem hibrida yang secara aktif mengorkestrasi deteksi *malware* berbasis DL pada *payload* email dan analisis anomali *network flow* menggunakan GNN, dilengkapi dengan mekanisme pertukaran intelijen ancaman yang otomatis.

DAFTAR PUSTAKA

[1] R. Sumargo dan H. Santoso, "Uncovering Malware Families Using Convolutional Neural Networks (CNN)," *Indonesian Journal of Artificial Intelligence and Data Mining (IJAIDM)*, vol. 7, no. 1, hlm. 97–103, 2024.

[2] U. W. Oluchukwu, A. S. Okwudili, A. D. Chinedu, E. C. Asogwa, dan A. K. Sylvanus, "Hybrid Machine Learning Algorithms for Email and Malware Spam Filtering: A Review," *European Journal of Theoretical and Applied Sciences*, vol. 2, no. 2, hlm. 76–86, 2024.

[3] L. Á. Redondo-Gutierrez *et al.*, "Detecting malware using text documents extracted from spam email through machine learning," dalam *Proceedings of the 2022 ACM Document Engineering Symposium (DocEng '22)*, New York, NY, USA, 2022, hlm. 1–2.

[4] F. Jáñez-Martino *et al.*, "Spam email classification based on cybersecurity potential risk using natural language processing," *Knowledge-Based Systems*, vol. 310, hlm. 112939, 2025, doi: 10.1016/j.knosys.2024.112939.

[5] S. Talukder dan Z. Talukder, "A Survey on Malware Detection and Analysis Tools," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 12, no. 2, hlm. 43–57, 2020.

[6] B. Konduri *et al.*, "Advancements and Challenges in Email Spam and Malware Filtering Utilizing AI and Machine Learning," *International Journal of Advanced Research in Computer and*

Communication Engineering, vol. 13, no. 4, hlm. 378–381, 2024, doi: 10.17148/IJARCCE.2024.13483.

[7] H. Rajeev dan M. Chakkravarthy, "Detection of Malware using Phishing Alarm," *Indian Journal of Artificial Intelligence and Neural Networking (IJAINN)*, vol. 4, no. 1, hlm. 1–4, 2023, doi: 10.54105/ijainn.A1077.124123.

[8] K. Thakur, M. L. Ali, M. A. Obaidat, dan A. Kamruzzaman, "A Systematic Review on Deep-Learning-Based Phishing Email Detection," *Electronics*, vol. 12, no. 21, hlm. 4545, 2023, doi: 10.3390/electronics12214545.

[9] O. Senouci dan N. Benaouda, "Enhancing Phishing Detection in Cloud Environments Using RNN-LSTM in a Deep Learning Framework," *Journal of Telecommunications and Information Technology*, vol. 1, no. 1, hlm. 1–9, 2025, doi: 10.26636/jtit.2025.1.1916.

[10] Q. Abu Al-Haija, A. Odeh, dan H. Qattous, "PDF Malware Detection Based on Optimizable Decision Trees," *Electronics*, vol. 11, no. 19, hlm. 3142, 2022, doi: 10.3390/electronics11193142.

[11] H. Zhang *et al.*, "A combined feature selection approach for malicious email detection based on a comprehensive email dataset," *Cybersecurity*, vol. 8, no. 1, hlm. 1–14, 2025, doi: 10.1186/s42400-024-00309-6.

[12] S. E. Adewumi dan U. D. Ani, "Impact of detection accuracy rates on phishing email spikes: Towards more effective mitigation," *Information Security Journal: A Global Perspective*, vol. 0, no. 0, hlm. 1–18, 2025, doi: 10.1080/19393555.2025.2469519.

[13] S. A. Aklani, H. Haeruddin, dan N. Putri, "Implementasi Mail Gateway Security dalam Meningkatkan Keamanan Email," *Journal of Information System Management (JOISM)*, vol. 5, no. 2, 2024.

[14] T. Rahmawati, N. Karna, S. Y. Shin, dan M. A. P. Putra, "Enhancing Network Security Through Real-Time Threat Detection with Intrusion Prevention System (Case Study on Web Attack)," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 10, no. 4, hlm. 1004–1020, 2024, doi: 10.26555/jiteki.v10i4.30380.

[15] J. Busch dan V. Tresp, "NF-GNN: Network Flow Graph Neural Networks for Malware Detection and Classification," *arXiv preprint arXiv:2103.03939*, 2021.

[16] M. Naseer *et al.*, "Obfuscated Malware Detection and Classification in Network Traffic Leveraging Hybrid Large Language Models and Synthetic Data," *Sensors*, vol. 25, no. 1, hlm. 202, 2025, doi: 10.3390/s25010202.

[17] A. Krajewska dan E. Niewiadomska-Szynkiewicz, "Clustering Network Traffic Using Semi-Supervised Learning," *Electronics*, vol. 13, no. 1, hlm. 94, 2024, doi: 10.3390/electronics13010094.

[18] M. Aljabri *et al.*, "Intelligent Techniques for Detecting Network Attacks: Review and Research Directions," *Sensors*, vol. 21, no. 21, hlm. 7070, 2021, doi: 10.3390/s21217070.

[19] Y. E. Suzuki dan S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," *Security Journal*, vol. 35, hlm. 1162–1182, 2022, doi: 10.1057/s41284-021-00318-x.

[20] A. H. Salem *et al.*, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data*, vol. 11, no.1, hlm. 105, 2024, doi: 10.1186/s40537-024-00957-y.

[21] P. Maniriho, A. N. Mahmood, dan M. J. M. Chowdhury, "A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges," *Future Generation Computer Systems*, vol. 130, hlm. 1–18, 2022, doi: 10.1016/j.fgcs.2021.11.018.