JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

Systematic Literature Review: Evolusi Ancaman Siber Dan Metode Deteksi *Malware* Di Sistem Operasi Android (2020–2025)

Nuansa Bening Aura Jelita[1], Herbert Siregar[1,*]

[1,2]Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Ilmu Komputer, Universitas Pendidikan Indonesia, Bandung, Indonesia
Email: [1]nbe.ning@upi.edu, [2]herbert@upi.edu
(*Email Corresponding Author: herbert@upi.edu)

Abstrak

Android sebagai sistem operasi *mobile* dominan menghadapi ancaman siber kompleks seperti *logic bombs, repackaging attack*, *banking trojans*, dan botnet. Metode deteksi berbasis *Machine Learning* (ML) dan *Deep Learning* (DL), seperti *Covalent Bond Strength Score* (akurasi 97,5%) dan *Zero Trust Architecture* (ZTA) untuk deteksi proaktif TTP, menunjukkan hasil yang menjanjikan. Analisis *graph-based* seperti *Triadic Suspicion Graph* (TSG) mencapai akurasi 99,9% dalam mendeteksi *banking trojans*, sementara metode *hybrid* berbasis NLP dan virtualisasi *ARM-based* membantu mengatasi eksploitasi *runtime* dan teknik penghindaran. Tantangan utama meliputi keterbatasan dataset *malware* dan serangan adversarial terhadap model AI. Studi ini menggunakan *Systematic Literature Review* (SLR) dengan pedoman PRISMA untuk memberikan gambaran komprehensif perkembangan deteksi *malware* Android. Temuan diharapkan mendukung pengembangan sistem keamanan yang lebih efektif dan adaptif.

Kata Kunci: Mobile *Operating System, Malware Detection, Android Malware, Systematic Literature Review,* PRISMA.

Abstract

Android, as the leading mobile operating system, faces increasingly complex cyber threats including logic bombs, repackaging attacks, banking trojans, and botnets. Detection methods leveraging Machine Learning (ML) and Deep Learning (DL), such as Covalent Bond Strength Score (97.5% accuracy) and Zero Trust Architecture (ZTA) for proactive TTP detection, have shown promising results. Graph-based analysis like Triadic Suspicion Graph (TSG) achieves up to 99.9% accuracy in detecting banking trojans, while hybrid NLP-based detection and ARM-based container virtualization address runtime exploits and evasive techniques. Challenges remain, including limited malware datasets and adversarial attacks on AI models. This study employs a Systematic Literature Review (SLR) guided by PRISMA to provide a comprehensive overview of Android malware detection advancements. The findings aim to support the development of more effective and adaptive security systems.

Keywords: *Mobile Operating System, Malware Detection, Android Malware, Systematic Literature Review, PRISMA.*

1. PENDAHULUAN

1.1 Latar Belakang

Peran sistem operasi sebagai pengelola sumber daya dan pelindung proses eksekusi menjadikannya komponen krusial dalam keamanan perangkat digital [1]. Android, sebagai sistem operasi *mobile* berbasis *open source* yang paling banyak digunakan di dunia, menawarkan fleksibilitas tinggi namun sekaligus membuka celah terhadap berbagai bentuk eksploitasi. Mos & Chowdhury (2020) menyoroti bahwa keterbukaan arsitektur Android memungkinkan penyisipan kode berbahaya ke dalam aplikasi sah melalui teknik seperti *repackaging*, serta penyalahgunaan *permission system* yang lemah.

Seiring berkembangnya teknologi dan meningkatnya integrasi perangkat *mobile* dalam kehidupan sehari-hari, *malware* Android terus berevolusi dengan kompleksitas teknik yang semakin tinggi dan canggih, seperti *logic bombs* yang memicu aktivitas berbahaya secara tersembunyi [3]. Selain itu, metode *repackaging attack* yang memungkinkan penyisipan kode berbahaya ke dalam aplikasi sah tanpa terdeteksi juga semakin banyak ditemukan [4].

Untuk mengatasi kenaikan ancaman ini, berbagai pendekatan deteksi *malware* telah dikembangkan, khususnya dengan memanfaatkan kemajuan dalam bidang *Machine Learning* (ML) dan *Deep Learning* (DL). Beberapa metode terbaru mencakup analisis urutan hibrida berbasis *Natural Language Processing* [5], serta kerangka kerja *ensemble learning* seperti *SEDMDroid* yang dapat meningkatkan akurasi klasifikasi *malware* secara signifikan [6].

Namun, efektivitas pendekatan-pendekatan ini masih dihadapkan pada berbagai tantangan, terutama dari teknik penghindaran deteksi dan eksploitasi *zero-day* yang belum diketahui sebelumnya [7]. Meskipun telah tersedia beberapa tinjauan literatur mengenai penerapan ML dalam deteksi *malware* Android [8], masih terdapat sejumlah aspek penting yang belum dieksplorasi secara mendalam. Misalnya, penggunaan kerangka kerja keamanan berbasis *Zero Trust Architecture* (ZTA) untuk memperkuat sistem proteksi aplikasi Android [9], serta pendekatan baru berbasis *Vision Transformers*, yang memiliki potensi tinggi dalam analisis *malware* [10].

Untuk menjawab berbagai tantangan tersebut dan memperjelas arah perkembangan teknologi deteksi *malware* Android, studi ini menggunakan metode utama *Systematic Literature Review* (SLR). Metode ini memungkinkan pengumpulan dan analisis berbagai studi secara sistematis dan transparan, sehingga dapat diperoleh gambaran menyeluruh mengenai tren, efektivitas, dan celah riset yang masih terbuka. Proses SLR ini mengikuti pedoman PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) untuk memastikan bahwa tahapan pencarian, seleksi, dan evaluasi artikel dilakukan secara runtut dan bisa dipertanggungjawabkan.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

Tinjauan ini akan mengeksplorasi berbagai pendekatan dalam mendeteksi *malware* Android dari tahun 2020 hingga 2025, termasuk teknik berbasis ML, DL, hingga pendekatan terbaru seperti *Vision Transformers* dan ZTA. Fokusnya tidak hanya pada metode deteksinya, tapi juga pada keefektifannya, tantangan yang dihadapi, dan celah penelitian yang masih terbuka. Harapannya, hasil review ini bisa jadi acuan yang kuat untuk pengembangan sistem keamanan Android yang lebih tangguh ke depannya.

1.2 Tujuan

Penelitian ini bertujuan untuk:

- **a.** Mengidentifikasi jenis ancaman siber yang umum pada sistem operasi Android (2020–2025).
- **b.** Menganalisis metode deteksi *malware* yang telah dikembangkan, khususnya berbasis *Machine Learning* dan *Deep Learning*.
- **c.** Mengevaluasi kelebihan, kelemahan, dan tantangan dari berbagai pendekatan deteksi *malware*.
- **d.** Memberikan rekomendasi untuk pengembangan sistem keamanan Android yang lebih efektif dan adaptif.

1.3 Pertanyaan Penelitian

Penelitian ini dirancang untuk menjawab tiga pertanyaan utama berikut:

RQ1. Apa saja jenis ancaman siber yang paling umum terjadi dalam ekosistem Android selama periode 2020–2025, dan bagaimana cara kerja *malware* dalam mengeksploitasi kerentanan sistem?

RQ2. Apa saja metode deteksi dan mitigasi yang telah dikembangkan dalam literatur terbaru, dan bagaimana pendekatan berbasis kecerdasan buatan dapat meningkatkan efektivitas identifikasi *malware*?

RQ3. Apa keunggulan dan kelemahan dari berbagai pendekatan deteksi yang telah ada, serta tantangan apa yang masih menjadi hambatan dalam pengembangan sistem keamanan Android yang lebih adaptif dan tangguh?

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan analisis deskriptif kualitatif yang berfokus pada penelaahan literatur terkait teknik dan perkembangan deteksi *malware* pada sistem operasi Android. Data diperoleh melalui kajian berbagai publikasi ilmiah yang mengangkat metode identifikasi *malware*, termasuk pendekatan berbasis ML, DL, serta kerangka kerja keamanan terkini. Proses telaah literatur dilakukan secara sistematis dengan mengikuti panduan PRISMA, guna memastikan hasil kajian tersusun secara runtut dan mampu merepresentasikan peta perkembangan riset dalam bidang ini secara menyeluruh.

2.1 *Search Process*

Dalam penelitian ini, proses pencarian literatur dilakukan secara sistematis melalui basis data Scopus, dengan menerapkan *query* yang disusun secara spesifik untuk menjangkau kajian terkini mengenai keamanan sistem operasi Android dalam konteks deteksi *malware*. *Query* yang digunakan meliputi:

"Operating System Security" OR "Android Security" AND "Android Malware"

"Operating System Security" AND "Mobile Security" OR "Android Security" AND "Android Malware"

Strategi pencarian ini bertujuan untuk menjaring sebanyak mungkin publikasi yang membahas topik keamanan sistem operasi Android, khususnya yang berfokus pada deteksi dan mitigasi *malware*. Seluruh hasil pencarian kemudian disaring lebih lanjut agar hanya literatur yang benar-benar relevan dan berkualitas yang dianalisis dalam penelitian ini.

2.2 *Inclusion and Exclusion Criteria*

Tabel 1. *Inclusion and Exclusion Criteria*

NO	Kriteria Inklusi	Kriteria Eksklusi
1.	Publikasi yang diterbitkan mulai tahun 2020 hingga 2025	Publikasi yang diterbitkan sebelum tahun 2020
2.	Penelitian yang berfokus pada bidang Ilmu Komputer (*Computer Science*), khususnya yang membahas keamanan sistem operasi	Studi yang tidak berfokus pada bidang Ilmu Komputer atau yang membahas topik di luar keamanan sistem operasi.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

NO	Kriteria Inklusi	Kriteria Eksklusi
3.	Artikel berupa dokumen penelitian asli (*research article*) yang dipublikasikan dalam jurnal ilmiah bereputasi dan tersedia secara *open access*	Dokumen selain artikel penelitian, seperti editorial, review, prosiding konferensi, laporan teknis, buku, atau artikel yang tidak tersedia secara terbuka (*non open access*).
4.	Artikel yang ditulis dalam bahasa Inggris	Artikel yang ditulis dalam bahasa selain Inggris

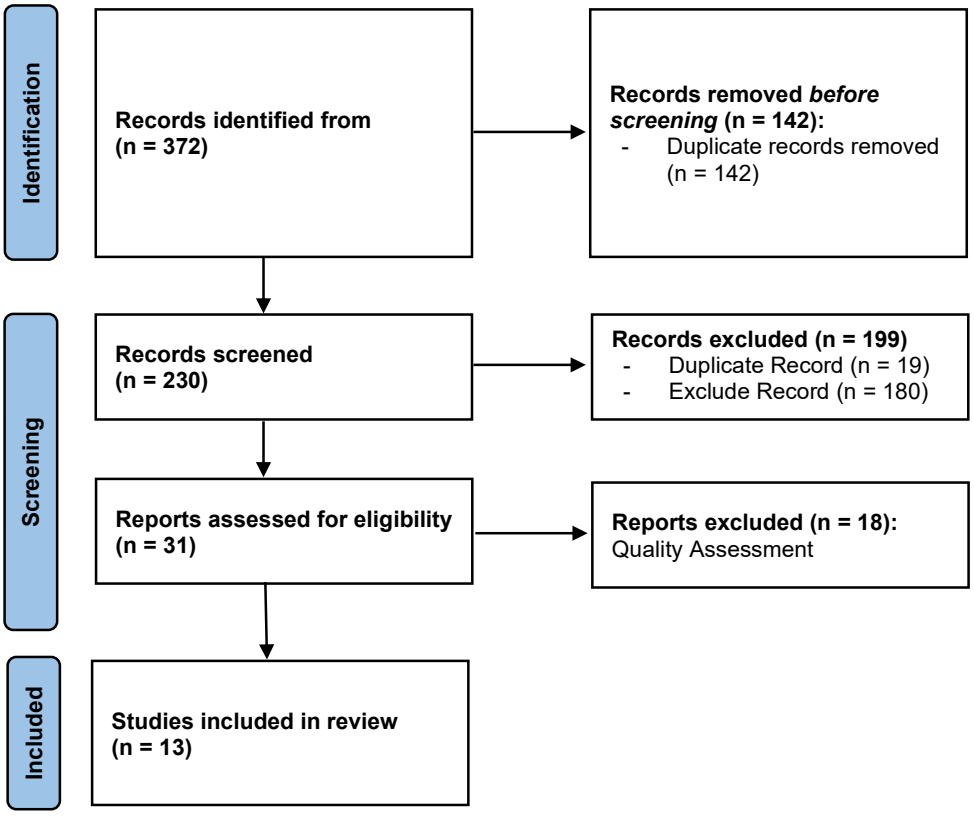
Pada tahap seleksi kelayakan ini, setiap artikel yang ditemukan melalui pencarian awal akan dievaluasi berdasarkan kriteria inklusi dan eksklusi tersebut. Pembatasan waktu publikasi mulai tahun 2020 dipilih agar kajian mencerminkan kemajuan dan inovasi terbaru dalam teknologi keamanan Android, khususnya dalam konteks deteksi *malware*. Fokus penelitian diarahkan pada literatur yang membahas secara eksplisit isu keamanan sistem operasi Android, sehingga artikel yang membahas topik lain atau kurang relevan tidak dimasukkan dalam analisis.

Kriteria bahasa juga menjadi pertimbangan penting untuk memastikan kelancaran proses analisis dan validasi data, sehingga hanya artikel berbahasa Inggris yang dipertimbangkan. Selain itu, penggunaan artikel yang tersedia secara *open access* memberikan kemudahan akses bagi peneliti dan meningkatkan transparansi proses penelitian. Pemilihan sumber yang berasal dari jurnal dan konferensi bereputasi juga bertujuan untuk menjaga mutu dan kredibilitas hasil tinjauan.

Penetapan kriteria inklusi dan eksklusi yang jelas dan terperinci ini sangat penting untuk menghindari bias seleksi dan memastikan bahwa literatur yang dianalisis benar-benar relevan dan berkualitas, sehingga hasil SLR ini dapat memberikan gambaran yang akurat dan komprehensif mengenai perkembangan dan tantangan dalam deteksi *malware* pada sistem operasi Android.

2.3 *Selection Process*

Seleksi literatur dilakukan secara bertahap untuk memastikan hanya publikasi yang benar-benar relevan dan berkualitas tinggi yang dianalisis lebih lanjut. Proses seleksi ini merujuk pada standar PRISMA, dimulai dari tahap identifikasi, *screening*, penilaian kualitas, hingga seleksi akhir artikel.



Gambar 1. *Selection Process* menggunakan PRISMA Diagram Flow

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

2.3.1 *Identification*

Pada tahap identifikasi, pencarian literatur dilakukan menggunakan database Scopus dengan kata kunci yang telah ditentukan. Awalnya, sebanyak 372 artikel berhasil dikumpulkan.

Selanjutnya, dilakukan penghapusan artikel duplikat menggunakan tool JabRef, yang mengeliminasi 142 artikel. Dengan demikian, tersisa 230 artikel unik yang siap untuk dilanjutkan ke tahap penyaringan berikutnya.

2.3.2 *Screening*

Pada tahap *screening*, dilakukan evaluasi mendalam terhadap judul dan abstrak dari 230 artikel yang telah melewati proses identifikasi dan penghapusan duplikasi. Tujuan dari tahap ini adalah untuk memastikan setiap artikel sesuai dengan kriteria inklusi dan eksklusi yang telah ditentukan, sehingga publikasi yang tidak relevan atau kurang memenuhi standar dapat disisihkan. Penilaian dilakukan secara cermat dan objektif agar hanya literatur yang benar-benar relevan yang dipertahankan untuk analisis lebih lanjut.

Dari keseluruhan artikel yang diperiksa, sebanyak 180 artikel tidak memenuhi persyaratan dan kemudian dikeluarkan dari kajian. Selain itu, ditemukan 19 artikel yang masih merupakan duplikat sehingga turut dihapus. Akibatnya, tersisa 31 artikel yang dianggap layak dan relevan untuk dilanjutkan ke tahap berikutnya, yaitu penilaian kualitas.

Tahap *screening* ini merupakan langkah krusial untuk memastikan fokus kajian tetap terjaga dan hanya mencakup literatur yang benar-benar mendukung tujuan penelitian tentang deteksi *malware* di sistem operasi Android.

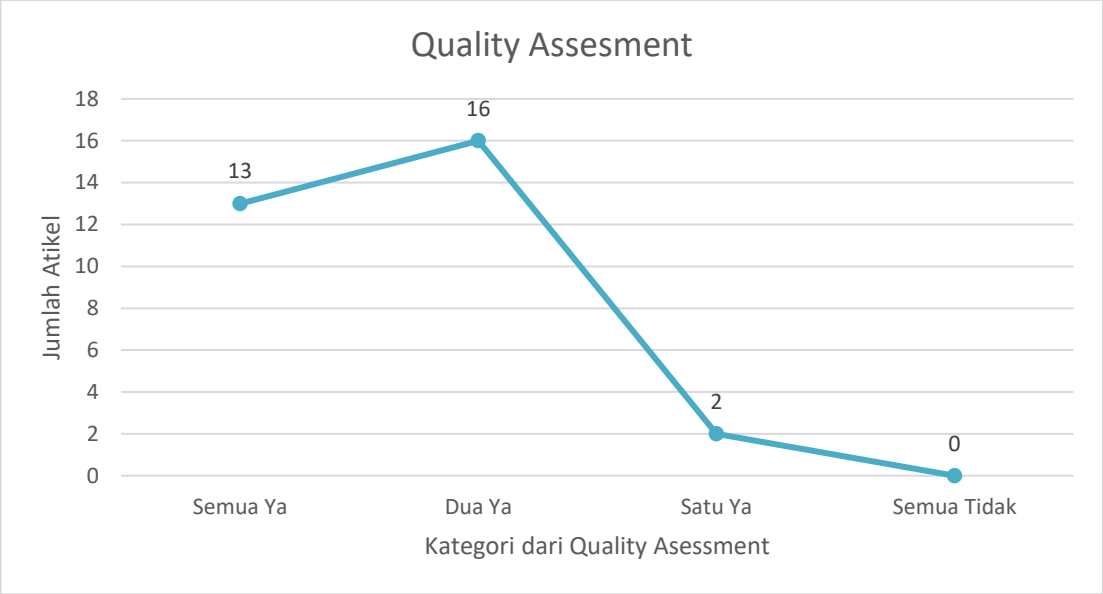
2.3.3 *Quality Assesment*

Pada tahap penilaian kualitas, artikel-artikel yang telah lolos tahap screening dievaluasi secara mendalam untuk memastikan bahwa hanya publikasi dengan kualitas tinggi dan relevansi yang kuat terhadap topik penelitian yang akan dianalisis lebih lanjut. Evaluasi ini bertujuan untuk menjaga standar akademik dan memastikan bahwa hasil analisis didasarkan pada data dan metodologi yang valid dan terpercaya. Penilaian kualitas dilakukan berdasarkan tiga kriteria utama yang dapat dilihat pada tabel 2. dibawah ini.

Tabel 2. *Quality Assessment Criteria*

QA#	Kriteria (Pertanyaan)	Penjelasan
QA1	Apakah artikel diterbitkan di sumber yang memiliki reputasi dan kredibilitas tinggi?	Artikel harus dipublikasikan di jurnal atau konferensi yang diakui secara akademis dan terindeks di database terpercaya seperti Scopus. Hal ini menjamin bahwa artikel telah melalui proses review yang ketat dan memenuhi standar kualitas ilmiah yang tinggi.
QA2	Apakah artikel relevan dengan topik deteksi *malware* pada sistem operasi Android?	Artikel yang dipilih harus secara jelas membahas teknik, metode, atau pendekatan yang digunakan untuk mendeteksi *malware* pada Android. Artikel yang membahas keamanan siber secara umum atau *malware* pada platform lain harus dipertimbangkan jika isinya dapat secara konseptual mendukung pemahaman deteksi *malware* pada Android.
QA3	Apakah artikel menyajikan metodologi yang jelas dan hasil yang dapat dipertanggungjawabkan?	Penelitian harus menjelaskan secara rinci metode yang digunakan dalam deteksi *malware*, seperti analisis statis, dinamis, atau penggunaan algoritma pembelajaran mesin. Metode yang dipaparkan harus transparan dan dapat direplikasi. Selain itu, artikel harus menyajikan hasil evaluasi yang lengkap dan terukur.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395



Gambar 2. Distribusi hasil *Quality Assesment*

Pada gambar 2. terlihat hasil evaluasi kualitas artikel berdasarkan tiga kriteria QA. Dari total 31 artikel yang dievaluasi, hanya 13 artikel yang memenuhi ketiga kriteria secara lengkap. Artikel-artikel ini dianggap memiliki kualitas dan relevansi terbaik untuk mendukung analisis lebih lanjut dalam penelitian *deteksi malware* pada sistem operasi Android. Oleh karena itu, hanya ke-13 artikel ini yang dipilih sebagai fokus utama untuk tahap ekstraksi data dan sintesis hasil.

Sementara itu, terdapat 16 artikel yang memenuhi dua dari tiga kriteria, namun artikel-artikel ini tidak dimasukkan sebagai referensi pendukung dalam penelitian ini karena dianggap belum memenuhi standar kualitas yang cukup untuk analisis mendalam. Sedangkan 2 artikel lainnya hanya memenuhi satu kriteria dan secara kualitas kurang memadai untuk dilanjutkan. Dengan seleksi yang ketat ini, penelitian memastikan bahwa hanya literatur dengan mutu terbaik yang dianalisis untuk menghasilkan temuan yang valid dan terpercaya

2.3.4 *Data Extraction*

Pada tahap data extraction, dilakukan pengumpulan dan pencatatan informasi penting dari artikel-artikel terpilih secara sistematis untuk menjawab pertanyaan penelitian terkait deteksi dan mitigasi *malware* pada sistem operasi Android. Proses ini menjadi dasar dalam menganalisis, merangkum, dan menginterpretasi temuan dari literatur yang dikaji.

Tabel 3. *List Data Extraction*

Data Extraction List Statement	Deskripsi
Identifikasi Publikasi Relevan	Mengumpulkan artikel yang secara eksplisit membahas deteksi *malware* Android, termasuk teknik dan pendekatan yang digunakan dalam mitigasi ancaman *malware*. Sehingga sesuai dengan fokus studi dan relevan.
Metode Evaluasi atau Eksperimen	Mendokumentasikan berbagai metode yang digunakan untuk deteksi *malware*, seperti analisis statis, dinamis, hybrid, serta penggunaan model ML atau DL. Selain itu, mencatat jenis dataset yang digunakan, teknik pelatihan, dan prosedur evaluasi yang diterapkan.
Hasil Evaluasi dan Kinerja	Mencatat hasil utama terkait efektivitas metode deteksi *malware*. Data ini penting untuk membandingkan keunggulan dan kelemahan masing-masing pendekatan.
Keterbatasan dan Ruang Lingkup Studi	Mengidentifikasi keterbatasan yang dilaporkan dalam tiap studi. Hal ini membantu memahami konteks dan cakupan temuan.
Implikasi dan Rekomendasi	Mencatat kesimpulan dan rekomendasi yang diajukan oleh penulis terkait pengembangan metode deteksi *malware* Android ke depan, termasuk peluang

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

Data Extraction List Statement	Deskripsi
	riset lanjutan, peningkatan algoritma, atau integrasi dengan sistem keamanan lainnya.

Kelima elemen ini menjadi panduan utama dalam proses ekstraksi data, sehingga analisis yang dilakukan dapat terstruktur dan fokus pada aspek-aspek penting dalam pengembangan teknik deteksi *malware* Android.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil SLR yang dilakukan dengan mengikuti pedoman PRISMA, peneliti berhasil mengidentifikasi 13 artikel relevan yang membahas deteksi *malware* pada platform Android selama periode 2020–2025. Artikel-artikel tersebut berasal dari jurnal dan konferensi bereputasi di bidang Ilmu Komputer, yang memberikan gambaran mendalam tentang perkembangan teknologi dan tantangan terkini.

Tabel 4. List Hasil Referensi

Penulis (Tahun)	Fokus Penelitian	Metode/Model Utama	Hasil Utama
Bai et al. (2021)	*Banking trojans*	*Triadic Suspicion Graph* (TSG)	Akurasi 99,9%, tahan adversarial
Gupta et al. (2024)	*Izin & system calls*	*Covalent Bond Strength Score*	Akurasi 97,5%
Park et al. (2020)	Virtualisasi & *sandboxing*	*A-Pot* (*ARM-based container*)	Efektif terhadap anti-emulator
Zhang et al. (2021)	*Hybrid* + NLP *detection*	*Static* + *dynamic* + NLP	Kuat hadapi *runtime injection*
Nazir et al. (2024)	*Zero Trust Android*	*Zero Trust Architecture* (ZTA)	Deteksi proaktif TTPs
Vu & Jung (2021)	CNN untuk Android *malware*	AdMat (CNN-on-matrix)	Deteksi pola visual berbasis matriks
Alecci et al. (2024)	*Logic bombs*	*Context-aware anomaly detection*	Deteksi dorman *activation*
Ma et al. (2022)	*Repackaging attack*	*Active warden analysis*	Evaluasi *proofing* tidak efektif
Seraj et al. (2024)	Android botnet	*Neural Network Detection*	Deteksi *zero-day* botnet
Zakeya et al. (2022)	Dataset *malware*	*Probing AndroVul*	Evaluasi dataset Drebin & AndroZoo
Seneviratne et al. (2022)	*Vision Transformer Malware*	*Self-supervised ViT*	Potensi deteksi otomatis berbasis ViT
Liu et al. (2020)	*Review* ML Android *malware*	*Literature Review*	Klasifikasi tren metode ML
Zhu et al. (2021)	*Ensemble learning*	*SEDMDroid (stacked ML)*	Akurasi 94,92%, kuat secara performa

Metode deteksi *malware* yang ditemukan dalam literatur ini dapat diklasifikasikan ke dalam lima kategori utama: *Machine Learning* dan *Deep Learning*, *Zero Trust Architecture* (ZTA), *graph analysis*, pendekatan hibrida (statis dan dinamis), serta virtualisasi dan *sandboxing*. Pembahasan hasil akan disusun secara sistematis berdasarkan tiga pertanyaan penelitian utama (RQ#) yang telah dirumuskan.

3.1 Menjawab Pertanyaan Penelitian

RQ1: Apa saja jenis ancaman siber yang paling umum terjadi dalam ekosistem Android selama periode 2020–2025, dan bagaimana cara kerja *malware* dalam mengeksploitasi kerentanan sistem?

Malware Android terus menunjukkan peningkatan kecanggihan dalam mengeksploitasi kerentanan sistem, dengan beberapa ancaman utama yang dominan dalam literatur terkini. Pertama, *Repackaging Attack* menjadi metode paling umum di mana penyerang memodifikasi aplikasi resmi dengan menyisipkan kode berbahaya, lalu mendistribusikannya kembali melalui kanal tidak resmi. Teknik ini berhasil mengelabui sistem deteksi berbasis *signature* dan mekanisme integritas aplikasi karena mempertahankan fungsionalitas asli aplikasi sambil menambahkan *payload* berbahaya [4].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

Kedua, *Logic Bombs* yang dirancang untuk tetap tidak aktif hingga kondisi spesifik terpenuhi, seperti lokasi geografis, waktu tertentu, atau aktivitas pengguna. Teknik ini menyulitkan deteksi karena hanya aktif dalam situasi terbatas. *Malware* jenis ini sering kali memanfaatkan teknik *context-aware evasion* untuk menghindari analisis statis [3].

Di sisi lain, eksploitasi izin aplikasi dan API sensitif semakin banyak ditemukan, di mana *malware* menyalahgunakan kombinasi izin yang diberikan pengguna dan pola eksekusi API kritis (misalnya akses SMS atau sensor perangkat) untuk memperoleh akses tidak sah ke data sensitif. Studi *SEDMDroid* menunjukkan bahwa metode tradisional berbasis *signature* gagal mendeteksi eksploitasi ini karena *malware* memanipulasi aliran data dinamis dan perubahan izin secara *runtime* [6].

Ancaman lain yang semakin mengkhawatirkan adalah botnet berbasis Android, di mana ribuan perangkat terinfeksi dikendalikan jarak jauh melalui server *Command and Control* (C&C) untuk melancarkan serangan DDoS, pencurian data massal, atau manipulasi transaksi finansial. Botnet ini sering menyusup melalui aplikasi palsu yang meniru layanan populer [7].

Selain itu, *Banking Trojans* menjadi ancaman kritis dengan teknik *overlay attack* yang menampilkan halaman login palsu di atas aplikasi perbankan resmi untuk mencuri kredensial pengguna. *Malware* ini mengeksploitasi API perbankan untuk mengakses informasi keuangan dan melakukan transaksi ilegal, sering kali dikombinasikan dengan teknik *privilege escalation* untuk memperoleh akses root [11]. Kombinasi ancaman-ancaman ini menggambarkan evolusi *malware* Android yang tidak hanya mengandalkan eksploitasi teknis, tetapi juga manipulasi psikologis pengguna dan penghindaran deteksi berbasis AI.

RQ2: Apa saja metode deteksi dan mitigasi yang telah dikembangkan dalam literatur terbaru, dan bagaimana pendekatan berbasis kecerdasan buatan dapat meningkatkan efektivitas identifikasi *malware*?

Literatur terbaru menunjukkan beragam metode deteksi dan mitigasi yang memanfaatkan kecerdasan buatan (AI) untuk meningkatkan efektivitas identifikasi *malware* Android. Salah satu metode inovatif adalah *Covalent Bond Strength Score*, yang menganalisis hubungan antara izin aplikasi dan *system calls*. Dengan menggabungkan teknik *static analysis* dan *dynamic analysis*, metode ini mampu mendeteksi pola eksploitasi *runtime manipulation* dan o*bfuscation* dengan akurasi mencapai 97,5% [12].

Pendekatan *Zero Trust Architecture* (ZTA) juga mulai digunakan dalam konteks keamanan Android. Sistem ini beroperasi dengan asumsi tidak ada entitas yang dipercaya secara default. Dengan dukungan AI, ZTA memantau perilaku aplikasi secara *real-time* dan mengidentifikasi pola serangan *Tactics, Techniques, and Procedures* (TTPs) sebelum eksploitasi terjadi, sehingga meningkatkan efektivitas pencegahan ancaman [9].

Metode *graph-based behavioral analysis* menjadi sangat efektif dalam mendeteksi *banking trojans*. Model seperti *Triadic Suspicion Graph* (TSG) menganalisis interaksi antar entitas dalam aplikasi untuk mengidentifikasi anomali, mencapai akurasi deteksi hingga 99,9% dengan tingkat *false positive* yang rendah [11].

Pendekatan *hybrid sequence-based detection* yang menggabungkan analisis urutan opcode statis dan *system calls* dinamis menggunakan *Natural Language Processing* (NLP) juga terbukti meningkatkan kemampuan deteksi *malware*, terutama dalam menghadapi perilaku *polymorphic* dan *runtime injection* yang kompleks [5].

Selain itu, platform berbasis virtualisasi dan *sandboxing*, seperti *A-Pot*, menggunakan *ARM-based containers* untuk menciptakan lingkungan analisis yang realistis dan tahan terhadap teknik anti-emulator yang sering digunakan oleh *malware* untuk menghindari deteksi. Integrasi *AI-driven behavioral analysis* dalam platform ini membantu mendeteksi anomali secara lebih efektif selama eksekusi aplikasi [13].

Secara keseluruhan, integrasi kecerdasan buatan dengan metode *hybrid* dan arsitektur keamanan modern menjadi kunci utama dalam menghadapi ancaman *malware* Android yang semakin kompleks.

RQ3: Apa keunggulan dan kelemahan dari berbagai pendekatan deteksi yang telah ada, serta tantangan apa yang masih menjadi hambatan dalam pengembangan sistem keamanan Android yang lebih adaptif dan tangguh?

Berbagai pendekatan deteksi *malware* Android yang berbasis *Machine Learning* dan *Deep Learning* telah berhasil meningkatkan akurasi klasifikasi *malware* secara signifikan. Contohnya, *framework SEDMDroid* mencapai akurasi 94,92%, sementara *AdMat* menggunakan *Convolutional Neural Networks* (CNN) pada matriks fitur aplikasi untuk mendeteksi pola berbahaya yang sulit dikenali oleh metode *signature* tradisional [6], [14].

Pendekatan *hybrid* yang menggabungkan analisis statis dan dinamis, diperkuat dengan NLP, mampu mengurangi tingkat *false positives* dan meningkatkan akurasi deteksi secara keseluruhan [5].

Arsitektur *Zero Trust* memungkinkan pemantauan perilaku aplikasi secara *real-time* dan deteksi proaktif terhadap ancaman melalui analisis TTPs, sehingga memberikan lapisan keamanan tambahan yang adaptif [9].

Model berbasis graph juga menunjukkan keunggulan dalam mendeteksi *banking trojans* dengan akurasi hingga 99,9% dan *false positive* yang rendah [11]. Namun, tantangan signifikan masih membayangi efektivitas sistem deteksi *malware* Android. *Malware* kini semakin menggunakan teknik penghindaran deteksi yang canggih, seperti anti-emulator, *anti-debugging*, *dynamic code loading*, dan teknik *obfuscation* yang kompleks, yang membuat deteksi menjadi semakin sulit [13].

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

Selain itu, masih terdapat keterbatasan dalam keberagaman dan kualitas dataset *malware* yang digunakan dalam pelatihan model AI. Sebagian besar penelitian masih mengandalkan dataset lama seperti Drebin dan AndroZoo, yang kurang representatif terhadap ancaman terbaru dan varian *malware* yang terus berkembang [15].

Lebih lanjut, serangan *adversarial* yang menargetkan model AI dapat mengecoh sistem deteksi dengan manipulasi input yang halus namun efektif, sehingga menimbulkan kerentanan baru yang perlu diatasi melalui teknik seperti *adversarial training* dan *robust learning* [11].

Untuk itu, pengembangan dataset yang lebih komprehensif dan representatif, integrasi metode *hybrid* yang lebih canggih, serta kolaborasi erat antara komunitas akademik dan industri sangat diperlukan untuk memperkuat sistem keamanan Android yang adaptif dan tangguh di masa depan.

4. KESIMPULAN

Berdasarkan hasil kajian *Systematic Literature Review* (SLR) terhadap 13 artikel utama periode 2020–2025, dapat disimpulkan bahwa *malware* Android mengalami evolusi signifikan dengan teknik eksploitasi kompleks seperti *logic bombs*, *repackaging*, *banking trojans*, *botnet*, serta penyalahgunaan izin dan API sistem. Pendekatan deteksi berbasis *Machine Learning* (ML), *Deep Learning* (DL), dan *Zero Trust Architecture* (ZTA) terbukti meningkatkan efektivitas identifikasi *malware*, didukung oleh model seperti *Covalent Bond Strength Score*, *Triadic Suspicion Graph* (TSG), dan *SEDMDroid* yang menunjukkan akurasi tinggi dalam klasifikasi ancaman. Namun, tantangan utama seperti keterbatasan dataset yang representatif, serangan *adversarial* terhadap model AI, dan teknik penghindaran deteksi yang semakin adaptif masih membayangi efektivitas metode-metode tersebut. Oleh karena itu, dibutuhkan pengembangan metode *hybrid* yang lebih tangguh, penerapan strategi deteksi proaktif berbasis *graph* dan *real-time monitoring*, serta kolaborasi antara komunitas akademik dan industri untuk memperkuat sistem keamanan Android secara berkelanjutan.

REFERENCES

[1] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating system concepts 10th edition*. Wiley, 2018. [Online]. Available: http://os-book.com/OS10/index.html

[2] A. Mos and M. M. Chowdhury, "Mobile security: A look into android," in *IEEE International Conference on Electro Information Technology*, 2020, pp. 638–642. doi: 10.1109/EIT48999.2020.9208339.

[3] M. Alecci, J. Samhi, L. Li, T. F. Bissyande, and J. Klein, "Improving logic bomb identification in android apps via context-aware anomaly detection," *IEEE Trans. Dependable Secur. Comput.*, vol. 21, no. 5, pp. 4735 – 4753, 2024, doi: 10.1109/TDSC.2024.3358979.

[4] H. Ma, S. Li, D. Gao, D. Wu, Q. Jia, and C. Jia, "Active warden attack: On the (in)effectiveness of android app repackage-proofing," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 3508–3520, 2022, doi: 10.1109/TDSC.2021.3100877.

[5] N. Zhang, J. Xue, Y. Ma, R. Zhang, T. Liang, and Y. an Tan, "Hybrid sequence-based android malware detection using natural language processing," *Int. J. Intell. Syst.*, vol. 36, no. 10, pp. 5770–5784, 2021, doi: 10.1002/int.22529.

[6] H. Zhu, Y. Li, R. Li, J. Li, Z. You, and H. Song, "SEDMDroid: An enhanced stacking ensemble framework for android malware detection," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 984–994, 2021, doi: 10.1109/TNSE.2020.2996379.

[7] S. Seraj, E. Pimenidis, M. Trovati, and N. Polatidis, "Zero-day android botnet detection using neural networks," *Neural Comput. Appl.*, 2024, doi: 10.1007/s00521-024-10818-7.

[8] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A review of android malware detection approaches based on machine learning," *IEEE Access*, vol. 8, pp. 124579–124607, 2020, doi: 10.1109/ACCESS.2020.3006143.

[9] A. Nazir, Z. Iqbal, and Z. Muhammad, "ZTA: A novel zero trust framework for detection and prevention of malicious android applications," *Wirel. Networks*, vol. 31, no. 4, pp. 3187 – 3203, 2024, doi: 10.1007/s11276-025-03935-1.

[10] S. Seneviratne, R. Shariffdeen, S. Rasnayaka, and N. Kasthuriarachchi, "Self-supervised vision transformers for malware detection," *IEEE Access*, vol. 10, pp. 103121–103135, 2022, doi: 10.1109/ACCESS.2022.3206445.

[11] C. Bai, Q. Han, G. Mezzour, F. Pierazzi, and V. S. Subrahmanian, "DBank: Predictive behavioral analysis of recent android banking trojans," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 3, pp. 1378–1393, 2021, doi: 10.1109/TDSC.2019.2909902.

[12] R. Gupta, K. Sharma, and R. K. Garg, "Covalent bond based android malware detection using permission and system call pairs," *Comput. Mater. Contin.*, vol. 78, no. 3, pp. 4283–4301, 2024, doi: 10.32604/cmc.2024.046890.

[13] J. Park, N. T. Chau, L. Nguyen-Vu, J. Yoon, and S. Jung, "A-pot: A comprehensive android analysis platform based on container technology," *IEEE Access*, vol. 8, pp. 199638–199645, 2020, doi: 10.1109/ACCESS.2020.3035774.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 227-235
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.395

[14] L. N. Vu and S. Jung, "Admat: A cnn-on-matrix approach to android malware detection and classification," *IEEE Access*, vol. 9, pp. 39680–39694, 2021, doi: 10.1109/ACCESS.2021.3063748.

[15] N. Zakeya, K. Ségla, T. Chamseddine, and B. B. Alvine, "Probing androvul dataset for studies on Android malware classification," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6883–6894, 2022, doi: 10.1016/j.jksuci.2021.08.033.