ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Antivirus security: A comprehensive overview of detection techniques, system architecture, and security-conscious defense measures.

Nainita Hansraj Nandeshwar , Dr. SM Ali

Department of Electronics and Telecommunications Engineering,
Anjuman College of Engineering and Technology, Nagpur

Abstract

Malware continues to threaten data integrity, privacy, and system availability in private, business, and government IT environments. Traditional signature-based antivirus programs are increasingly being superseded by polymorphic, fileless, and zero-day malware. This article examines the evolution of antivirus security, summarizing signature-based, heuristic, behavioral, and machine learning detection methods, as well as proactive vulnerability analysis using sources such as the National Vulnerability Database (NVD). Starting with a summary of a proposed antivirus system and an expanded review of current literature, this article presents a multi-layered system architecture, a real-time detection and response workflow, and a comparative evaluation of detection techniques. Furthermore, it discusses the risks of attackers circumventing security measures, the rise of next-generation antivirus (NGAV) and endpoint detection and response (EDR) platforms, and ongoing challenges such as minimizing false positives and resource-efficient deployment. The study concludes that a hybrid, vulnerability-focused architecture that combines multiple detection levels offers the most resilient path to adaptive, resource-efficient protection against current and emerging cyber threats.

Keywords: Antivirus, malware detection, heuristic scanning, behavioral analysis, machine learning, vulnerability assessment, NVD/CVE, endpoint detection and response

1. Introduction

The increasing reliance of individuals, businesses, and governments on digital infrastructure has made cybersecurity a central concern. Malware—including viruses, worms, Trojans, ransomware, and spyware—remains among the most persistent threats to computer systems, compromising data integrity, privacy, and overall system functionality (Aboaoja et al. 2022). Antivirus software is specifically designed to prevent infections, detect suspicious activity, and assure users that a system is not compromised.

Signature-based detection, the foundation of early antivirus programs, compares file contents against a database of known malware patterns. While this approach is computationally efficient, it is structurally incapable of detecting malware it has not yet identified. This leaves systems vulnerable to zero-day and polymorphic attacks (Bazrafshan et al. 2013). This limitation has driven research toward heuristic scans, behavioral analysis, and—more recently—machine learning and deep learning models that can generalize beyond known signatures (Bensaoud, Kalita, and Bensaoud 2024; Souri and Hosseini 2018).

Besides reactive detection, unpatched software vulnerabilities represent an equally significant attack surface. The integration of vulnerability information from databases such as the National Vulnerability Database (NVD) enables security systems to proactively identify exploitable vulnerabilities before they are exploited by attackers (Li 2023; Kritikos et al. 2019). This review article summarizes the technical foundations, comparative strengths, and open research questions of modern antivirus security. It is based on a proposed master's thesis on "Antivirus Security," which is significantly expanded upon by current specialist literature and industry publications.

2. Literature review

The literature on virus protection and malware defense can be divided into several overlapping research strands: traditional and heuristic detection, behavior-based and host-based analysis, classification using machine learning and deep learning, ransomware detection, malware defense for mobile devices/Android, vulnerability analysis, robustness against attackers, and the emerging class of next-generation antivirus and endpoint detection and response (EDR) platforms.

2.1 Signature-based and heuristic recognition

Bazrafshan et al. (2013) provide an early and widely cited comparison of heuristic malware detection techniques. They contrast API call sequences and N-gram-based features with classical signature matching and find that while heuristic approaches have a higher false-positive rate, they offer broader coverage of unknown variants. Souri and Hosseini (2018) extend this comparison through a systematic analysis of data mining techniques used for both signature-based and behavior-based detection. They conclude that hybrid pipelines generally outperform detectors using only one technique.

2.2 Behavioral and host-based analysis

Jacob, Debar, and Filiol (2008) established one of the first formal taxonomies for behavior-based malware detection. They argued that runtime behavior signals—such as process startup, registry modification, and network activity—are more resistant to obfuscation than static code features. Building on this, Sworna et al. (2023) show that natural language processing techniques applied to host and event logs can uncover anomalous behavior sequences indicative of compromise. Zhong et al. (2024) investigate graph neural network approaches to intrusion detection that model host and network behavior as relational graphs—an approach directly applicable to behavior-based antivirus modules.

2.3 Approaches to machine learning and deep learning

The trend toward learned detection models is well documented. Bensaoud, Kalita, and Bensaoud (2024) investigate deep learning-based malware detection systems for Windows, Linux, and mobile platforms, highlighting the ongoing challenges regarding model interpretability and robustness against attacks. Brown, Gupta, and Abdelsalam (2024) apply automated machine learning (AutoML) to deep learning-based malware detection, thereby reducing the manual effort required to optimize detection pipelines. Manikandaraja, Aaby, and Pitropakis (2023) demonstrate that simple preprocessing and feature engineering techniques can significantly improve the accuracy of resource-efficient machine learning detectors without the overhead of large neural architectures. Hai et al. (2023) propose an image-based malware representation in combination with an EDR pipeline that converts binary executables into image tensors for convolutional classification.

2.4 Ransomware-specific detection

Due to its severe impact on operations, ransomware detection has attracted particular attention. Li, Wang, and Shu (2022) combine feature selection with particle swarm optimization to improve the accuracy of behavior-based ransomware classification. Singh et al. (2020) apply a minimal redundancy, maximum relevance (mRMR) feature selection method to enable earlier detection before file encryption is complete. Mousavi et al. (2022) directly address the challenges posed by ransomware attacks, demonstrating that ensemble learning increases resilience against ransomware variants designed to evade a single classifier.

2.5 Malware detection for mobile devices and Android devices

Given the widespread use of mobile applications, a substantial body of literature addresses Android-specific malware. Naseer et al. (2017) provide a systematic overview of static analysis tools for Android applications, while Razgallah et al. (2021) and Sihag, Vardhan, and Singh (2021) examine detection and hardening techniques,

respectively. Both studies indicate that permission-based and static analysis capabilities remain vulnerable to code obfuscation and dynamic loading. Chen, Ding, and Wagner (2023) directly address the obsolescence of models and propose a continuous learning framework that regularly adapts Android malware classifiers to the evolving threat landscape.

2.6 Vulnerability analysis and databases

A comprehensive antivirus solution must go beyond reactive detection and include proactive vulnerability management. Li (2023) systematically maps the structure and metadata gaps of vulnerability databases, enabling more robust queries of sources such as the NVD. Kritikos et al. (2019) evaluate vulnerability scanners and databases using a criteria-based framework and find that no single tool meets all criteria regarding completeness and timeliness. Mirtaheri et al. (2025) apply lean generative AI models to predict the severity of vulnerabilities directly from current NVD entries, thus providing a means for the automated prioritization of patching measures.

2.7 Robustness against attacks and evasion mechanisms

As detection models evolve, so do evasion techniques. Chatzoglou et al. (2023) empirically demonstrate that even old, well-cataloged malware families can bypass modern commercial antivirus programs using simple repackaging tricks, highlighting that signature recency alone is insufficient. Yan et al. (2023) and Macas, Wu, and Fuertes (2024) investigate attacks on machine learning-based classifiers and catalog threats through evasion, manipulation, and model extraction, as well as the corresponding defense techniques, including adversarial training and ensemble diversity.

2.8 Next-generation antivirus and endpoint detection and response

Industry practice has focused on multi-layered platforms that combine prevention with continuous monitoring. Next-generation antivirus (NGAV) extends signature matching with machine learning and behavioral heuristics to block threats before execution. Endpoint detection and response (EDR) provides continuous telemetry, forensic logging, and automated containment for threats that evade prevention (CrowdStrike 2025; Palo Alto Networks n.d.). Maniriho, Mahmood, and Chowdhury (2024) situate this industry trend in the academic literature by examining malware detection techniques on Windows and identifying the integration of prevention and response layers as an open field of research—directly motivating the multi-layered architecture proposed in Section 3 of this review.

2.9 Summary of the most important literature

Table 1 summarizes representative studies on the detection paradigms discussed above and highlights for each the technique, the most important contribution and a reported limitation.

Author(s) / Year	Detection approach	Most important contribution	Reported restriction
Bazrafshan et al. (2013)	Heuristic recognition	API call and N-gram heuristic features were compared with signature methods.	High rate of false positive results with obfuscated code
Jacob, Debar and Filiol (2008)	Behavioral recognition	An established taxonomy for behavior-based malware detection has been proposed.	The taxonomy lacked empirical validation in real-world systems.
Souri and Hosseini (2018)	Data mining / Machine learning	Systematic review comparing signature-based and behavior-based data mining detectors	Limited coverage of methods from the Deep Learning era
Y. Li et al. (2022)	Feature selection + PSO	Improved accuracy of	Evaluated based on a

		ransomware classification through particle swarm feature optimization	narrowly defined selection of ransomware families
Singh, Sihag and Vardhan (2020)	mRMR feature selection	Reduced functional redundancy for earlier ransomware detection	Early detection still lags behind with fast-encrypting variants.
Mousavi et al. (2022)	Ensemble learning	Improved robustness of ransomware detectors against attack attempts	The ensemble overhead increases the running costs.
Aboaoja et al. (2022)	ML-based recognition (overview)	Cataloged open questions and challenges in ML-based malware detection	Identifies gaps without proposing a uniform solution.
Bensaoud, Kalita and Bensaoud (2024)	Deep Learning (Overview)	Investigation of deep learning methods on Windows, Linux and mobile platforms	The interpretability of the notes remains unclear.
Chatzoglou et al. (2023)	Evasive analysis	Empirically investigated how traditional malware bypasses modern antivirus programs.	The results are limited to tested commercial engines.
Yan et al. (2023)	Adversarial ML	Investigation of attack and defense methods for malware classifiers	Defense systems often trade accuracy for robustness.
Kritikos et al. (2019)	Vulnerability analysis	Evaluation of tools and databases for vulnerability scanning using criteria-based frameworks	No single instrument met all the evaluation criteria.
Mirtaheri et al. (2025)	Generative AI evaluation	Lightweight generative models were used to predict the severity of security vulnerabilities based on NVD data.	The accuracy of the model depends on the completeness of the NVD metadata.

Table 1. Summary of representative literature on antivirus and malware detection techniques.

3. Problem definition

While traditional antivirus software is effective against known threats through signature-based detection, it cannot keep pace with the rapid evolution of malware variants, zero-day attacks, and attackers' evasion techniques (Chatzoglou et al. 2023; Yan et al. 2023). At the same time, unpatched software vulnerabilities serve as entry points that attackers can exploit independently of direct malware injection. Many existing antivirus solutions also lack integrated vulnerability analysis based on authoritative sources such as the NVD (Kritikos et al. 2019). The absence of a unified, adaptive framework that combines real-time malware detection with proactive vulnerability analysis exposes both home users and businesses to the risk of security breaches, financial losses, and reputational damage.

4. Review of the system architecture

Figure 1 illustrates the detection paradigms described in Section 2 in a multi-layered block diagram for an antivirus security system. This system combines signature-based, heuristic, behavior-based, and real-time monitoring modules with a proactive vulnerability analysis module. Incoming files, processes, and network traffic are simultaneously routed to the individual detection modules. The results are aggregated by a decision and correlation module, which determines whether an object should be quarantined, flagged as potentially dangerous, or confirmed as safe. A parallel vulnerability analysis module compares installed software against NVD/CVE databases and feeds both the

decision module and a reporting dashboard. This provides users with a unified overview of active threats and latent vulnerabilities.

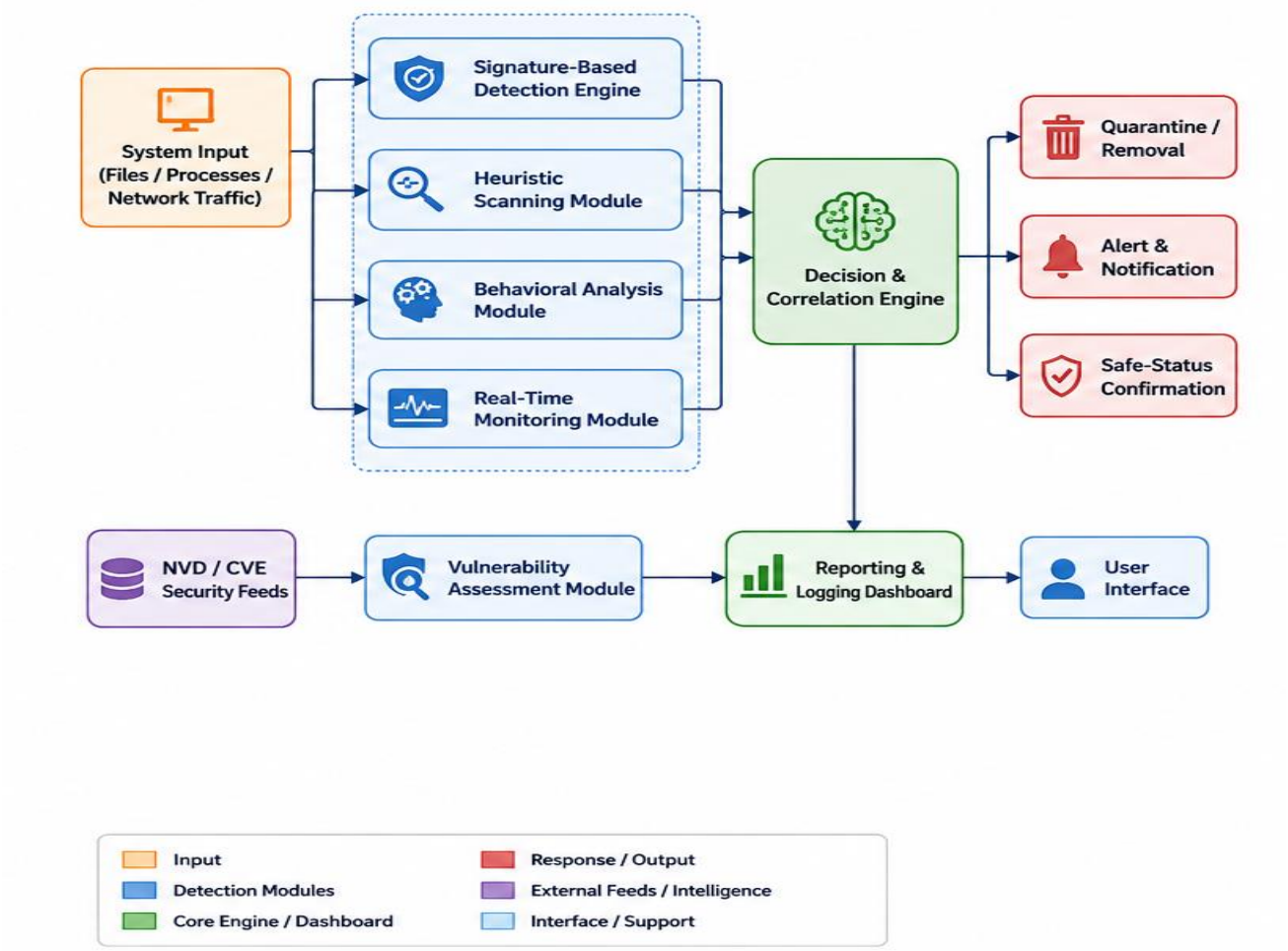

Figure 1. Block diagram of the proposed architecture of the antivirus security system.

This architecture reflects the consensus in the reviewed literature that no single detection technique is sufficient on its own (Souri and Hosseini 2018; Aboaoja et al. 2022): Signature matching offers speed and precision against known threats, heuristic and behavior-based layers extend coverage to unknown variants, and the vulnerability assessment module closes the gap created by purely reactive detection.

5. Real-time detection and response workflow

Figure 2 illustrates the operational flow of the investigated system when accessing a file or process. The real-time scan engine first checks for an exact signature match; if a match is found, the object is immediately quarantined. Otherwise, the object is heuristically examined for suspicious code patterns. Suspicious objects undergo behavioral analysis and sandbox monitoring, while non-suspicious objects are marked as safe. Confirmed malicious behavior triggers an alert and quarantine measures. Unconfirmed objects are checked against NVD/CVE entries for vulnerabilities before the result is logged in the reporting dashboard. This tiered pipeline reflects the escalation strategy described by Jacob, Debar, and Filiol (2008) and the early detection focus of Singh et al. (2020), balancing the detection delay with the risk of false positives at each stage.

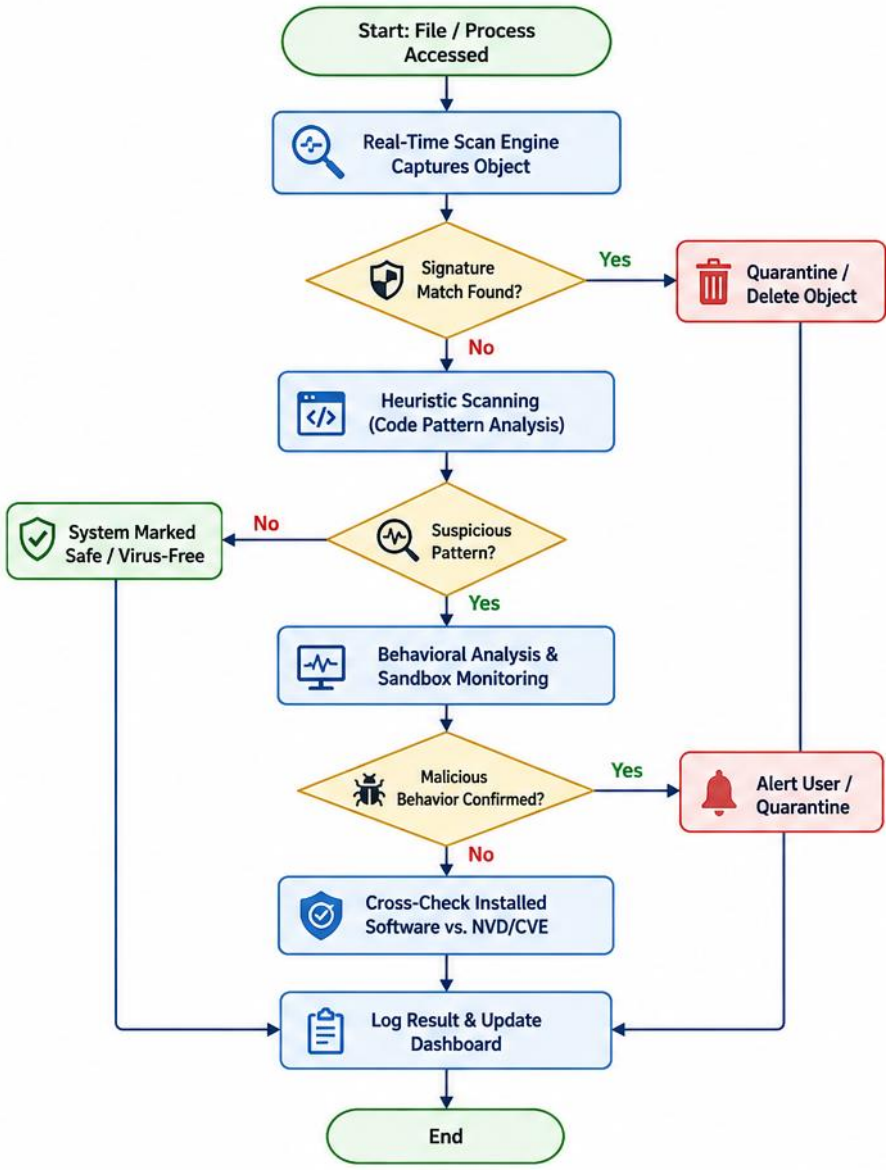

Figure 2. Flowchart of the real-time malware detection and response process.

6. Comparative analysis of detection techniques

Table 2 summarizes the strengths and weaknesses of each detection paradigm discussed in the literature review, with particular emphasis on suitability for zero-day attacks – an important distinguishing feature identified in the studies examined (Bazrafshan et al. 2013; Bensaoud, Kalita and Bensaoud 2024; Yan et al. 2023).

Technology	Detection	Basic strengths	Weaknesses / Suitability for zero-day exploits
Signature-based	Exact byte/hash pattern match with a database of known malware	Fast, low false positive rate, minimal resource consumption	Ineffective against zero-day and polymorphic malware
Heuristic scanning	Rule-based review of the	Detects variants of known	Tendency towards more

	code structure and statement patterns	malware families	frequent false alarms; rules must be constantly adapted.
Behavioral analysis	Runtime monitoring of process, file, and API call activity	Effective against unknown and fileless threats	Increased computational effort; delayed detection until execution
Machine learning / Deep learning	Statistical or learned patterns from marked sets of characteristics	Adapts to changing threats; high zero-day potential	Vulnerable to attacks from adversaries; requires large, annotated datasets
Vulnerability analysis (NVD/CVE)	Comparison of installed software with known CVE entries	Proactively closes exploitable security gaps before infection occurs.	Active malware cannot be detected; this depends on the database's freshness.
Next Generation EDR / AV	Combined prevention, telemetry and forensic response	Provides transparency and options for response if preventive measures fail.	Higher implementation complexity and higher operating costs

Table 2. Comparative analysis of antivirus detection methods.

No single technology is superior in all criteria. Signature-based detection remains unsurpassed in terms of speed and precision against known threats, but offers no protection against novel malware. Behavioral and machine learning methods close this gap, but at the cost of increased computational effort and vulnerability to evasion attempts. This balancing of advantages and disadvantages justifies the layered architecture with multiple engines presented in Section 4.

7. Integration of the vulnerability analysis

In addition to active malware, unpatched software vulnerabilities represent an independent and often underestimated attack surface. Integrating a vulnerability analysis module—by querying installed software configurations against NVD and CVE databases—enables the system under review to inform users about exploitable vulnerabilities even without an active infection (Li 2023). Mirtaheri et al. (2025) further demonstrate that generative AI methods can automate the prioritization of these findings by directly predicting vulnerability severity based on current NVD metadata, thus reducing the manual prioritization effort. This proactive layer complements the reactive detection mechanisms described above and reflects the industry-wide shift from purely preventive antivirus protection to comprehensive endpoint risk management (CrowdStrike 2025).

8. Challenges and future direction

Despite significant progress, some challenges remain unresolved in the literature reviewed:

- Minimizing false alarms: Heuristic and behavior-based systems must be carefully calibrated to avoid alarm fatigue, which can lead users to ignore genuine warnings (Bazrafshan et al. 2013).
- Robustness against attacks: Machine learning-based detectors remain vulnerable to evasion, poisoning, and model extraction attacks, requiring continuous investment in adversarial training and ensemble defenses (Yan et al. 2023; Macas, Wu and Fuertes 2024).
- Lightweight deployment: Behavioral and deep learning modules must be optimized to avoid impacting system performance, especially on resource-constrained endpoints (Manikandaraja, Aaby and Pitropakis 2023).
- Up-to-dateness of the vulnerability database: The effectiveness of each module integrated into NVD/CVE depends on the completeness and up-to-dateness of the underlying data feed (Kritikos et al. 2019).
- Cross-platform coverage: Extending unified detection and vulnerability frameworks from desktop operating systems to mobile and IoT endpoints remains an active area of research (Maniriho, Mahmood and Chowdhury 2024; Sihag, Vardhan and Singh 2021).

Future work should explore closer integration between continuous EDR-style telemetry and generative AI-powered vulnerability analysis, as well as standardized benchmarks that jointly assess detection accuracy, false positive rate, and vulnerability assessment coverage within a single framework.

9. Conclusion

This overview traces the evolution of antivirus security from signature-based detection methods through heuristic, behavioral, and machine learning to the increasing importance of proactive vulnerability analysis. The literature unanimously shows that no single detection method offers complete protection: signature-based systems are precise but reactive; heuristic and behavioral methods enhance protection but are prone to false positives and require more computation; and machine learning models offer adaptability, but this is limited by the risk of attacks. A multi-layered architecture—such as the one presented in Section 4—that combines these detection strategies with continuous vulnerability analysis using sources like the NVD represents the most secure way to protect user data, privacy, and system integrity in private, business, and government IT environments.

References

(Chicago author-date style)

1. Aboaoja, Fatima A., Anazida Zainal, Fuad A. Ghaleb, Bander Ali Saleh Al-rimy, Taiseer Abdalla Elfadil Eisa, and Asmaa H. Elnour. 2022. “Problems, challenges, and future directions in malware detection: A survey.” Applied Sciences 12 (17): 8482.
2. Bazrafshan, Zahra, Hashem Hashemi, Seyed Mehdi Hazrati Fard, and Ali Hamzeh. 2013. “An overview of heuristic malware detection techniques.” In: Proceedings of the 5th Conference on Information and Knowledge Technology (ICT), pp. 113–120. Shiraz: IEEE.
3. Bensaoud, Ahmed, Jugal Kalita, and Mahmoud Bensaoud. 2024. “An overview of malware detection using deep learning.” arXiv preprint.
4. Brown, Austin, Maanak Gupta, and Mahmoud Abdelsalam. 2024. "Automated machine learning for malware detection using deep learning." Computers & Security 137: 103582.
5. Chatzoglou, Efstratios, Georgios Karopoulos, Georgios Kambourakis, and Zisis Tsiatsikas. 2023. “Bypassing Antivirus Detection: Old-School Malware, New Tricks.” arXiv preprint.
6. Chen, Yizheng, Zhoujie Ding, and David Wagner. 2023. “Continuous Learning for Android Malware Detection.” In: Proceedings of the 32nd USENIX Security Symposium, pp. 1127–1144. Anaheim, CA: USENIX Association.
7. CrowdStrike. 2025. “EDR vs. NGAV: How to assess the differences.” CrowdStrike Cybersecurity 101. Accessed September 2, 2026.
8. Hai, Tran Hoang, Vu Van Thieu, Tran Thu Duong, Hoang Hai Nguyen, and Eui-Nam Huh. 2023. “A proposed novel endpoint detection and response system with image-based malware detection.” IEEE Access 11: 122859–122875.
9. Jacob, Gregoire, Herve Debar, and Eric Filiol. 2008. “Behavioral detection of malware: From a survey to an established taxonomy.” Journal in Computer Virology 4 (3): 251–266.
10. Joshi, Yashwant Kumar. 2023. “A comprehensive overview of malware detection techniques.” Proceedings of the ACM Symposium on Applied Computing.
11. Kritikos, Kyriakos, Kostas Magoutis, Manos Papoutsakis, and Sotiris Ioannidis. 2019. “A survey of tools and databases for vulnerability assessment for cloud-based web applications.” Array 3–4: 100011.

12. Li, Xin. 2023. “The anatomy of a vulnerability database: A systematic mapping study.” Journal of Systems and Software 201: 111679.

13. Li, Yuxin, Xiaohan Wang, and Hui Shu. 2022. “Behavioral Ransomware Classification Using Feature Selection and Particle Swarm Optimization.” Information Sciences 610: 1101–1119.

14. Macas, Mayra, Chunming Wu and Walter Fuertes. 2024. “Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Enabled Cybersecurity Systems.” Expert Systems with Applications 238: 122223.

15. Manikandaraja, Aravindhan, Peter Aaby, and Nikolaos Pitropakis. 2023. “RapidRift: Elementary techniques for improving machine learning methods for malware detection.” Computers 12 (10): 195.

16. Maniriho, Pascal, Abdun Naser Mahmood, and Mohammad Jabed Morshed Chowdhury. 2024. “A systematic literature review on Windows malware detection: techniques, research questions, and future directions.” Journal of Systems and Software 209: 111921.

17. Mirtaheri, Seyedeh Leili, et al. 2025. “Automated prediction of vulnerability scores through resource-efficient generative AI.” Computers & Security 148: 103982.

18. Mousavi, Seyed Mohammad, and colleagues. 2022. “Mitigating Adversarial Evasion Attacks of Ransomware through Ensemble Learning.” IEEE Access 10: 63465–63478.

19. Naseer, Sibgha, et al. 2017. “Static analysis of Android apps: A systematic review.” Information and Software Technology 88: 67–95.

20. Palo Alto Networks. n.d. “What is EDR compared to antivirus?” Palo Alto Networks Cyberpedia. Retrieved September 2, 2026.

21. Razgallah, Asma, Raphael Khoury, Sylvain Halle, and Kobra Khanmohammadi. 2021. “An overview of malware detection in Android apps: Recommendations and perspectives for future research.” Computer Science Review 39: 100358.

22. Shetty, Nahush, et al. 2021. “A review article on malware detection techniques.” International Journal of Advanced Trends in Computer Science and Engineering 10 (3): 2156–2162.

23. Sihag, Vikas, Manu Vardhan, and Pradeep Singh. 2021. “An overview of Android application and malware hardening.” Computer Science Review 39: 100365.

24. Singh, Karan, and colleagues. 2020. “Minimum Redundancy Maximum Relevance Method for Ransomware Early Detection.” Journal of Computer Virology and Hacking Techniques 16: 331–342.

25. Souri, Alireza, and Rahil Hosseini. 2018. “A current overview of malware detection approaches using data mining techniques.” Human-Centric Computing and Information Sciences 8 (1): 3.

26. Sworna, Zarrin Tasnim, et al. 2023. “NLP methods in host-based intrusion detection systems: A systematic review.” Computers & Security 132: 103349.

27. Yan, Shuai, Jiaqi Ren, Wei Wang, Limin Sun, Wei Zhang, and Qingyun Yu. 2023. “An overview of adversarial attack and defense methods for malware classification in cybersecurity.” IEEE Communications Surveys & Tutorials 25 (1): 467–496.

28. Zhong, Meng, et al. 2024. “An overview of graph neural networks for intrusion detection systems: methods, trends, and challenges.” Computers & Security 141: 103821.