Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.074164

REVIEW

Malware Detection and AI Integration: A Systematic Review of Current Trends and Future Directions

M. Mohsin Raza[1,#], Muhammad Umair[1,#], Imran Arshad Choudhry[1], Muhammad Qasim[1], Muhammad Tahir Naseem[2,*], Mamoona Naveed Asghar[3], Daniel Gavilanes[4,5,6,7], Manuel Masias Vergara[4,8,9] and Imran Ashraf[10,*]

[1]Faculty of Information Technology & Computer Science, University of Central Punjab, Lahore, 54782, Punjab, Pakistan
[2]Department of Electronic Engineering, Yeungnam University, Gyeongsan-si, 38541, Republic of Korea
[3]School of Computer Science, University of Galway, Galway, H91 TK33, Ireland
[4]Higher Polytechnic School, Universidad Europea del Atlantico, Isabel Torres 21, Santander, 39011, Spain
[5]Engineering Research and Innovation Group, Universidad Internacional Iberoamericana, Campeche, 24560, Mexico
[6]Department of Projects, Universidade Internacional do Cuanza, Cuito, EN250, Bie, Angola
[7]Research Group on Foods, Nutritional Biochemistry and Health, Fundacion Universitaria Internacional de Colombia, Bogota, 11131, Colombia
[8]Universidad Internacional Iberoamericana, Arecibo, PR 00613, USA
[9]Universidad de La Romana, La Romana, 22000, Republica Dominicana
[10]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-si, 38541, Republic of Korea

*Corresponding Authors: Muhammad Tahir Naseem. Email: nmtahir@yu.ac.kr; Imran Ashraf. Email: imranashraf@ynu.ac.kr

[#]These authors contributed equally to this work

Received: 04 October 2025; Accepted: 10 December 2025; Published: 30 March 2026

ABSTRACT: Over the past decade, the landscape of cybersecurity has been increasingly shaped by the growing sophistication and frequency of malware attacks. Traditional detection techniques, while still in use, often fall short when confronted with modern threats that use advanced evasion strategies. This systematic review critically examines recent developments in malware detection, with a particular emphasis on the role of artificial intelligence (AI) and machine learning (ML) in enhancing detection capabilities. Drawing on literature published between 2019 and 2025, this study reviews 105 peer-reviewed contributions from prominent digital libraries including IEEE Xplore, SpringerLink, ScienceDirect, and ACM Digital Library. In doing so, it explores the evolution of malware, evaluates detection methods, assesses the quality and limitations of widely used datasets, and identifies key challenges facing the field. Unlike existing surveys, this work offers a structured comparison of AI-driven frameworks and provides a detailed account of emerging techniques such as hybrid detection frameworks and image-based analysis. The findings indicate that AI-based models trained on diverse, high-quality datasets consistently outperform conventional methods, particularly when supported by feature engineering, explainable AI and a multi-faceted strategy. The review concludes by outlining future research directions, including the need for standardized datasets, enhanced adversarial robustness, and the integration of privacy-preserving mechanisms in malware detection systems.

KEYWORDS: Cybersecurity; machine learning; malware dataset; malware detection; feature selection; deep learning; explainable AI (XAI)

1 Introduction

In the wake of the digital age, the world is faced with increasingly malicious activities, which refer to actions deliberately carried out to harm individuals or businesses, most commonly including viruses, worms, rootkits, ransomware, phishing attacks, advanced persistent threats (APTs), and botnets. Malware, which first emerged in the 1970s, began as a basic but destructive type of software capable of compromising sensitive information. Over the years, it has evolved significantly, fueled by factors such as state sponsorship and financial backing from powerful entities. Today, these threats target critical sectors, including healthcare, finance, education, and defense, leading to substantial financial losses, operational disruptions, and global ramifications. The alarming rise in malware attacks, particularly in the aftermath of the COVID-19 pandemic, underscore the urgent need for robust cybersecurity measures to counter these dangers [1–3]. According to AV-TEST, the independent IT-Security Institute, the number malware count over the last decade has increased dramatically, with millions of new malware samples being detected each year. This surge reflects the growing sophistication and diversity of cyber threats. According to Statista Technology Market Outlook, cybercrime is expected to skyrocket in coming years (Fig. 1).

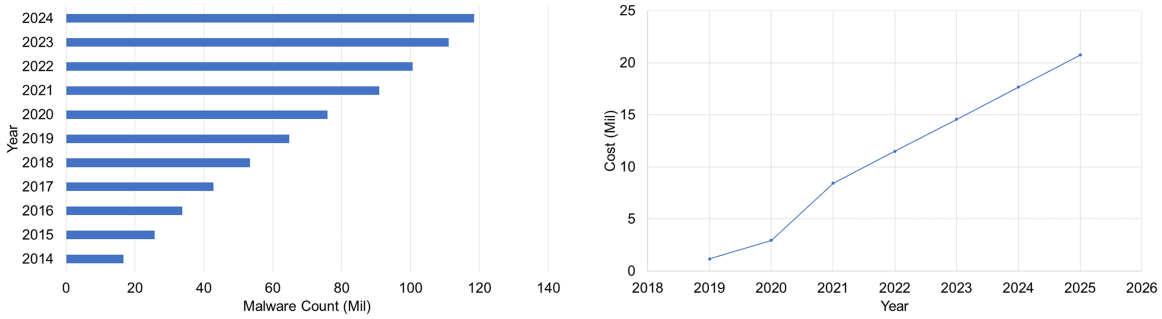

Figure 1: (Left) Malware counts (in Millions) over the last decade (Source: av-atlas.org), and **(Right)** Financial losses due to cyber crime (Source: Statista.com)

The evolution of malware has created a pressing need for significant advancements in cybersecurity to combat the increasing risks posed by sophisticated threats. Organizations are investing substantial resources to strengthen their defense systems, focusing on proactive strategies such as zero-trust architectures, continuous monitoring, and threat intelligence. Traditional detection techniques like signature-based, heuristic-based, behavior-based, and machine learning (ML)-based techniques have proven effective to some extent but the rise of AI-driven malware requires these methods to adapt and evolve significantly. Advanced technologies such as deep learning, hybrid detection frameworks, and real-time monitoring are becoming essential for enhancing detection accuracy and ensuring resilience against evolving threats [4–6]. AI-powered automation reduces reliance on manual interventions, enabling cybersecurity professionals to concentrate on more strategic tasks. These solutions also scale effectively to meet the demands of large and complex network infrastructures, ensuring consistent protection across diverse environments. By integrating machine learning (ML) models and intelligent automation, AI-driven tools optimize resource allocation and reduce response times, making them essential components of modern cybersecurity strategies [7,8].

Another critical factor influencing the effectiveness of malware detection is the quality and comprehensiveness of datasets. State-of-the-art datasets provide the foundation for training an advanced detection models, offering diverse and representative malware samples, including novel and emerging variants. These datasets enable the development of ML and deep learning (DL) models capable of identifying intricate patterns and detecting zero-day threats. Additionally, they facilitate rigorous evaluation and benchmarking

of detection techniques, ensuring their applicability and robustness in real-world scenarios. High-quality datasets also promote collaborative research and innovation, empowering the cybersecurity community to devise adaptive and scalable solutions to counter increasingly sophisticated malware [9].

Despite the increasing number of reviews addressing malware detection, there remains a gap in critically synthesizing recent advancements through the lens of AI integration, dataset robustness, resource constraints, automation, explainability, and hybrid methodologies. Prior surveys have often focused narrowly on specific detection scheme or failed to assess the scalability and interpretability of AI models, limiting their practical application.

This paper addresses these limitations by conducting a structured review of malware detection research from 2019 to 2025. It uniquely integrates an analysis of AI-powered detection techniques with a critical examination of publicly available datasets, explores the intersection of interpretability and accuracy in detection models, and highlights future research opportunities in privacy-preserving analysis, adversarial robustness, automation and explainable AI.

1.1 Rationale for This Survey

Several surveys have explored aspects of malware detection (e.g., behavior analysis, heuristic strategies, or deep learning methods), but they often lack a unified framework that connects malware evolution, dataset quality, and AI integration. Table 1 of this paper offers a comparative evaluation of such existing works, highlighting their limited focus on research reproducibility, dataset accessibility, or explainability of detection models. Thus, a comprehensive and up-to-date survey is warranted to guide future research in AI-driven malware detection.

Table 1: Comparative analysis of key malware detection surveys with respect to research questions addressed in the study

Ref.	Year	Malware evolution trend	Dataset analysis	AI integration	Privacy/ Trustworthiness
[10]	2019	No	No	No	No
[11]	2019	No	No	No	No
[12]	2021	No	No	No	No
[13]	2021	Yes	No	No	No
[14]	2023	Yes	No	No	No
[15]	2023	No	No	Yes	No
[16]	2024	Yes	No	No	No
[17]	2024	No	No	No	No
[18]	2024	Yes	No	No	No
[19]	2024	Yes	No	Yes	No
[20]	2024	Yes	No	No	No
[21]	2024	Yes	No	No	No
[22]	2024	No	No	Yes	No
[23]	2024	No	Yes	No	No
[24]	2025	No	No	Yes	Yes
[25]	2025	Yes	No	Yes	No

(Continued)

Table 1 (continued)

Ref.	Year	Malware evolution trend	Dataset analysis	AI integration	Privacy/ Trustworthiness
[26]	2025	Yes	No	No	No
[27]	2025	Yes	No	Yes	No
[28]	2025	Yes	No	No	No
[29]	2025	No	No	Yes	No
[30]	2025	Yes	No	Yes	No
[31]	2025	Yes	No	Yes	No

The reviewed survey papers provide varying degrees of coverage for the specified research questions. While improvements in detection techniques are often discussed in surveys, the efficacy of AI-driven cybersecurity solutions in comparison to conventional techniques and crucial elements like datasets and AI-driven solutions are still not thoroughly explored. As illustrated in Table 1, only study [23] has addressed dataset limitations or the interpretability of detection models, and none offered a comprehensive analysis integrating explainable AI, privacy-preserving concept, and dataset accessibility except [24]. Furthermore, several existing surveys lack focus on hybrid frameworks or adversarial robustness, which are crucial for modern threat landscapes. This highlights the need for a more integrated and critical review, as attempted in this study, that not only summarizes detection techniques but also addresses emerging challenges and future directions in AI-based malware detection.

1.2 Paper Structure

The remainder of this paper is organized as follows: Section 2 presents the research methodology, including the research questions, objectives, and shortlisting criteria. The historical evolution and recent trends in malware development are discussed in Section 3. Various detection techniques and AI integration are examined in Section 4. Different datasets and their impact on model performance are critically analyzed in Section 5, while Section 6 synthesizes the findings across the reviewed studies. Moreover, Section 7 discusses practical implications, limitations, and future directions, while Section 8 concludes the study. The structure of the paper is illustrated in Fig. 2.

2 Research Methodology

This study adopts a structured and transparent literature review methodology modeled after systematic review practices. Although not strictly following the PRISMA framework, the review employs its core principles, namely, predefined research questions, rigorous selection criteria, transparent reporting, and reproducibility, to ensure methodological robustness.

The review was conducted in five main stages: (1) formulation of research questions (RQs), (2) derivation of research objectives (ROs), (3) design of a detailed search strategy, (4) application of inclusion/exclusion criteria and article shortlisting, and (5) synthesis and thematic analysis of selected literature. The overarching goal is to evaluate state-of-the-art malware detection framework in the context of AI integration, dataset reliability, and emerging challenges.

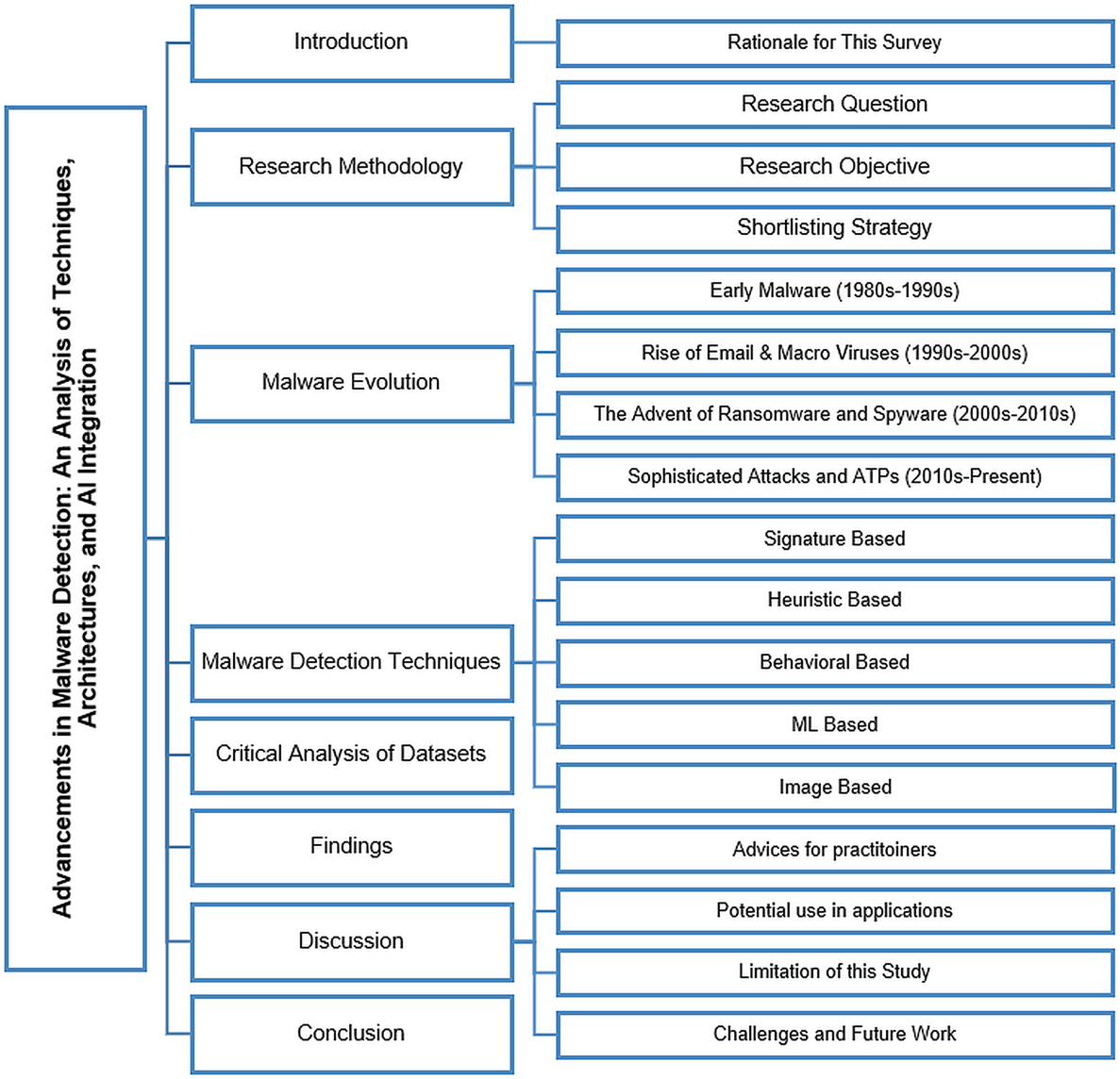

Figure 2: Structure of the review with section and subsection headings

2.1 Research Question

The review was guided by the following research questions:

i. What emerging trends have defined malware evolution in the past decade, and in what ways do they challenge existing detection approaches?
ii. How are current malware detection techniques addressing modern and evasive malware threats?
iii. In what ways do malware dataset characteristics influence the reproducibility and reliability of detection models?
iv. How can AI-driven cybersecurity solutions be applied to improve the scalability and efficiency of malware detection systems?

2.2 Research Objectives

Derived from the RQs, the objectives of this review are:

i. Analyze and document the major trends and patterns in the development and propagation of malware over the last ten years.
ii. Evaluate the effectiveness of hybrid frameworks, image-based models, and adversarial defense mechanisms in countering evasive malware.
iii. Analyze the impact of synthetic, federated, and multimodal datasets on malware detection, with emphasis on dataset quality, reproducibility, and fairness.
iv. Explore how automation, evolutionary algorithms, XAI, and privacy-preserving AI can be integrated for scalable, transparent, and resilient malware detection.

2.3 Shortlisting Strategy

This review follows a structured methodology inspired by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, making deliberate adaptations to suit the cybersecurity and AI research domain. The cybersecurity literature is more dispersed over a variety of venues (journals, conferences, seminars, and technical reports) than the medical or clinical research where PRISMA first appeared. Consequently, a strict PRISMA protocol was not entirely applicable. Instead, its core principles of transparency, reproducibility, and systematic filtering were preserved, while modifications were introduced to accommodate domain-specific characteristics. The search strategy targeted high-quality peer-reviewed publications from January 2019 to October 2025 (Fig. 3). The search process was designed to maximize coverage across both general and specialized digital libraries. In addition to IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier (ScienceDirect), and IJCERT, supplementary sources such as Wiley Online Library, MDPI, and arXiv were also consulted to broaden scope (Fig. 2). To avoid overlooking relevant work, backward and forward snowballing was performed on included studies.

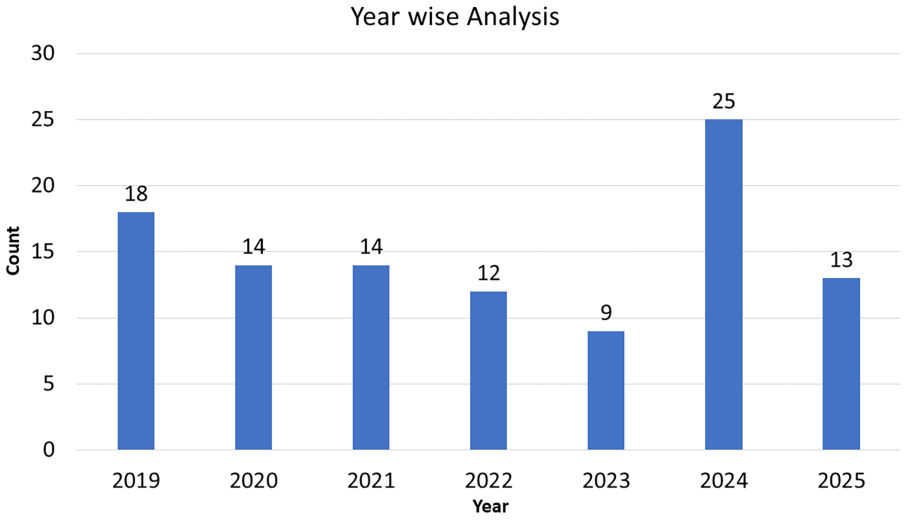

Figure 3: Year-wise distribution of articles referenced in this study

The following Boolean-based search strings were employed:

("malware detection" OR "malicious software detection" OR "threat detection" OR "cyber defense") AND ("machine learning" OR "artificial intelligence" OR "deep learning" OR "neural networks") AND ("dataset" OR "feature selection" OR "explainable AI" OR "adversarial robustness" OR "hybrid model") AND ("cybersecurity" OR "cyberphysical systems" OR "IoT security") AND ("feature selection" OR "XAI" OR "hybrid model")

2.3.1 Inclusion Criteria

Peer-reviewed studies (2019–2025) focusing on malware detection using AI, ML, or hybrid design, including works analyzing datasets or proposing comparative frameworks.

2.3.2 Exclusion Criteria

Non-English studies, editorials, short abstracts without technical depth, and duplicates. Fig. 4 illustrates the PRISMA flow diagram followed in this review, PRISMA checklists can be found in the Supplementary Materials. A total of 526 records were identified from five digital libraries (IEEE Xplore, ACM DL, Springer-Link, Elsevier, and IJCERT). After removing duplicates and screening abstracts, 268 full-text articles were assessed for eligibility. Of these, 52 were excluded due to lack of technical depth, duplication, or access restrictions. Ultimately, 105 studies were included in the final qualitative synthesis. To ensure consistency and reduce selection bias, two independent reviewers assessed each article. Disagreements were resolved by a third reviewer. The inter-rater agreement was measured using the Kappa Coefficient, yielding a value of 0.81, indicating substantial agreement. The H-index values were obtained using the Scopus and Google Scholar databases, where available, and reflect the cumulative impact of each source venue. This quality measure complements the inclusion criteria (e.g., publication years, peer-reviewed status), contributing to the robustness of the review methodology. Publisher-wise distribution of the papers is shown in Table 2.

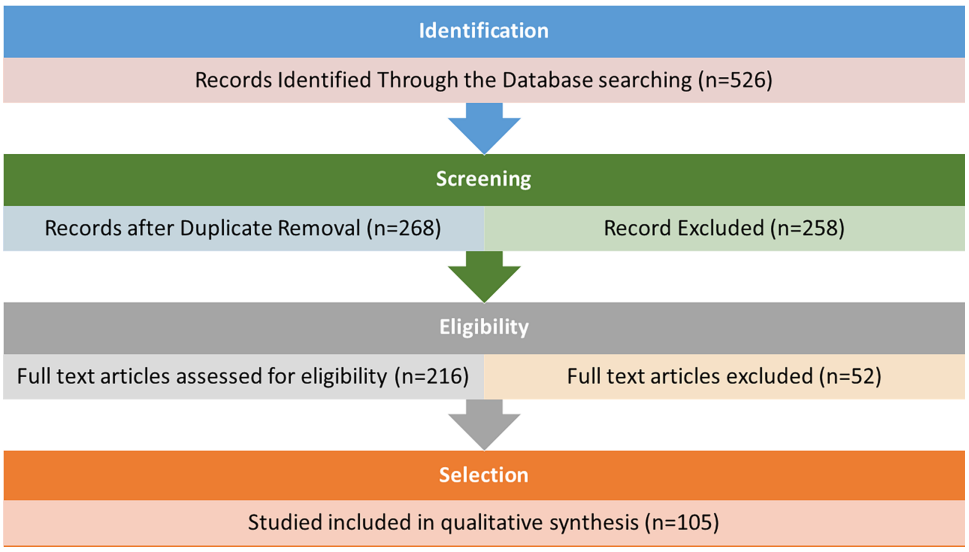

Figure 4: PRISMA flow diagram illustrating the study selection process for this systematic review

Table 2: Publisher-wise distribution of papers with corresponding references

Publisher	Count	References
IEEE Transactions	41	[12,18,20,22,24–28,32–63]
Elsevier	9	[11,14–16,23,64–67]
ACM	7	[21,29,68–72]
Springer	5	[31,73–76]
MDPI	4	[30,77,78]
CMES	3	[79–81]
IJCERT	1	[82]
Misc	35	[10,13,17,19,83–113]
Total	105	

2.4 Quality Assessment and Weighting

To promote transparency and credibility in the synthesis process, each of the included studies was assessed using a Quality–Evidence–Impact (QEI) scoring framework. QEI is not an international standard but this framework offers a structured method to evaluate methodological quality (*Quality*), empirical support (*Evidence*), and real-world relevance (*Impact*), and has been adopted from existing literature [114–116]. As shown in Table 3, each dimension was scored on a three-point scale, with a maximum score of nine points. Studies with QEI scores of 7 or higher were considered high-quality evidence and were given greater weight when interpreting findings and developing the analytical framework. This systematic assessment indicates (Fig. 5) that approximately 62% of the reviewed studies exhibit strong methodological rigor and validated results, ensuring that the conclusions of this review are based on a solid and diverse empirical foundation.

Table 3: Quality–Evidence–Impact (QEI) scoring of selected studies

Study	Q	E	I	Total/Category	Study	Q	E	I	Total/Category
[21]	2	2	2	6 (Moderate)	[32]	3	3	3	9 (High)
[36]	3	3	2	8 (High)	[37]	2	2	2	6 (Moderate)
[39]	2	3	2	7 (High)	[48]	3	2	2	7 (High)
[59]	3	3	3	9 (High)	[64]	3	3	3	9 (High)
[58]	3	2	2	7 (High)	[67]	2	3	2	7 (High)
[94]	2	2	2	6 (Moderate)	[98]	3	3	3	9 (High)
[100]	3	3	2	8 (High)	[103]	2	2	2	6 (Moderate)
[106]	2	3	2	7 (High)	[107]	2	2	3	7 (High)
[99]	2	2	2	6 (Moderate)	[57]	3	3	2	8 (High)
[52]	3	3	2	8 (High)	[20]	3	3	2	8 (High)
[65]	2	2	2	6 (Moderate)	[82]	2	2	2	6 (Moderate)
[101]	2	3	2	7 (High)	[33]	2	2	2	6 (Moderate)
[83]	3	2	2	7 (High)	[34]	2	2	2	6 (Moderate)
[35]	3	2	2	7 (High)	[77]	2	2	2	6 (Moderate)
[85]	2	2	3	7 (High)	[84]	3	2	2	7 (High)
[86]	2	2	2	6 (Moderate)	[112]	3	2	2	7 (High)
[87]	2	2	2	6 (Moderate)	[41]	2	2	2	6 (Moderate)
[40]	3	2	2	7 (High)	[88]	2	2	2	6 (Moderate)

(Continued)

Table 3 (continued)

Study	Q	E	I	Total/Category	Study	Q	E	I	Total/Category
[89]	2	2	2	6 (Moderate)	[93]	2	2	3	7 (High)
[42]	2	2	2	6 (Moderate)	[92]	2	2	2	6 (Moderate)
[45]	3	2	2	7 (High)	[44]	2	2	2	6 (Moderate)
[91]	2	2	2	6 (Moderate)	[90]	2	2	2	6 (Moderate)
[43]	2	2	2	6 (Moderate)	[68]	3	2	2	7 (High)
[46]	3	2	2	7 (High)	[96]	3	2	2	7 (High)
[75]	2	2	2	6 (Moderate)	[95]	3	2	2	7 (High)
[49]	3	2	2	7 (High)	[67]	2	3	2	7 (High)
[97]	2	2	2	6 (Moderate)	[47]	2	2	2	6 (Moderate)
[71]	3	3	3	9 (High)	[60]	3	3	2	8 (High)
[66]	2	3	2	7 (High)	[108]	2	2	2	6 (Moderate)
[56]	2	2	2	6 (Moderate)	[61]	2	2	2	6 (Moderate)
[62]	2	3	2	7 (High)	[110]	2	3	2	7 (High)

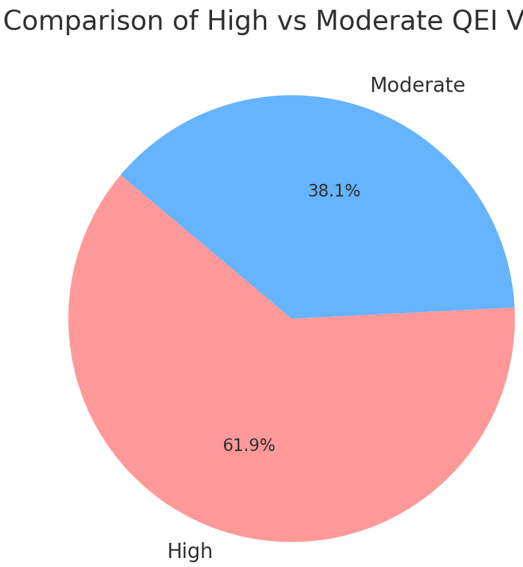

Figure 5: QEI Score comparison over Higher Vs. moderate

2.4.1 Scoring Criteria

Each study included in the review received a score using three important dimensions:

- **Quality (Q):** Assesses the methodological rigor of each study, where 1 = weak or unclear methods, 2 = moderate rigor, and 3 = robust and reproducible methodology.
- **Evidence (E):** Evaluates the strength of empirical validation, where 1 = minimal or descriptive validation, 2 = comparative or simulation-based validation, and 3 = strong empirical testing with benchmark datasets.
- **Impact (I):** Reflects the degree of real-world applicability, where 1 = theoretical only, 2 = potential applicability, and 3 = demonstrated real-world or cross-domain relevance.

3 Malware Evolution

Malicious software, also known as malware, has undergone significant evolution over the past decade. Notable factors in this evolution are increased sophistication, diversification of attack vectors, and advanced obfuscation techniques. It is very important to understand the evolution of malware (Fig. 6) for developing effective cybersecurity measures.

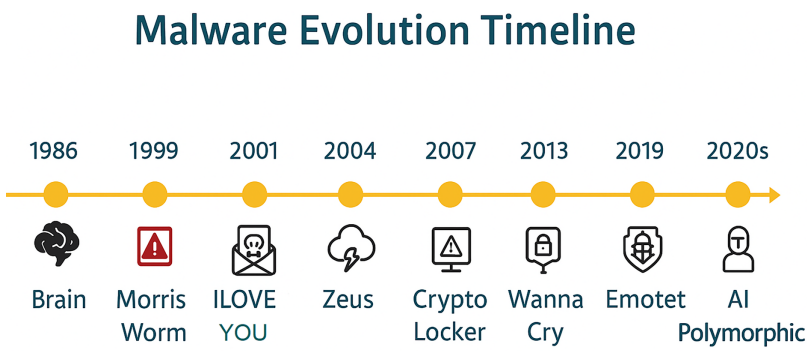

Figure 6: Malware evolution timeline over the years

3.1 Early Malware (1980–1990s)

The initial wave of malware mostly consisted of viruses and worms. These early forms of malware were relatively simple in design and spread primarily through infected floppy disks and internet connections. In this regard, Brain virus (1986) comes to the mind first, which was the first International Business Machines Corporation (IBM) PC virus. Morris worm (1988) is also another initial virus which caused widespread disruption across the early internet [117].

3.2 The Rise of Email and Macro Viruses (1990–2000s)

In 1990s email and office productivity software gained widespread recognition. This adoption also brought creation of macro viruses and email-borne malware. The Melissa virus (1999) and the ILOVEYOU worm (2000) exploited email systems. They propagated rapidly and caused significant financial and operational damage [118].

3.3 The Advent of Ransomware and Spyware (2000–2010s)

The early 2000 s saw the emergence of ransomware. It was a highly lethal kind of malware, which encrypts the victim's data and it was erased on demand of a ransom from user. AIDS trojan (PC Cyborg Virus) is considered as one of the first ransomware attacks ever which was released via floppy disk in 1989. Ransomware has a long history but it could not make impact till 2000 s. This was likely due to the challenges associated with collecting ransom payments. However, with the emergence of cryptocurrencies in 2010, such as Bitcoin, and soon spread globally. Meanwhile, spyware, which collects information from users without their knowledge, has also become a common threat, like Gator and CoolWebSearch [119].

3.4 Sophisticated Attacks and APTs (2010s–Present)

The last decade has seen an exponential increase in the sophistication of malware. Advanced Persistent Threats (APTs) are highly targeted and prolonged attacks. They are often sponsored by state [120]. In this regard, Stuxnet (2010) is one of the prominent attacks, which targeted Iranian nuclear facilities. Another notable attack is Sony Pictures hack (2014) [121].

Modern malware is gradually utilizing artificial intelligence (AI) and machine learning techniques to boost its effectiveness. These technologies allow malware to adapt to the situation and evade traditional detection methods by learning from previous detection attempts. They accordingly modifying their signature and behavior.

4 Malware Detection Techniques

Recent reports are evident that significant efforts are required to counter these malware attacks. Malware detection is a critical first step in combating malware attacks, as identification and detection are essential before implementing any measures to eliminate it. Following are basic malware detection techniques which have also evolved over the years.

4.1 Signature-Based Techniques

Signature-based malware detection remains one of the earliest and most widely deployed techniques in cybersecurity, owing to its precision and efficiency in identifying known threats. Simple Flow diagram of traditional signature base techniques is depicted in Fig. 7. By comparing binary patterns, code fragments, or network traces against a database of predefined signatures, these systems can deliver rapid detection with relatively low false positive rates. This reliability has preserved their relevance, especially in enterprise environments where response speed and operational stability are critical. However, as malware authors increasingly employ polymorphism, obfuscation, and zero-day exploits, the standalone effectiveness of signature-based solutions is diminishing. These evolving evasion strategies highlight the reactive nature of signature matching and underline the necessity for continual enhancement of this approach.

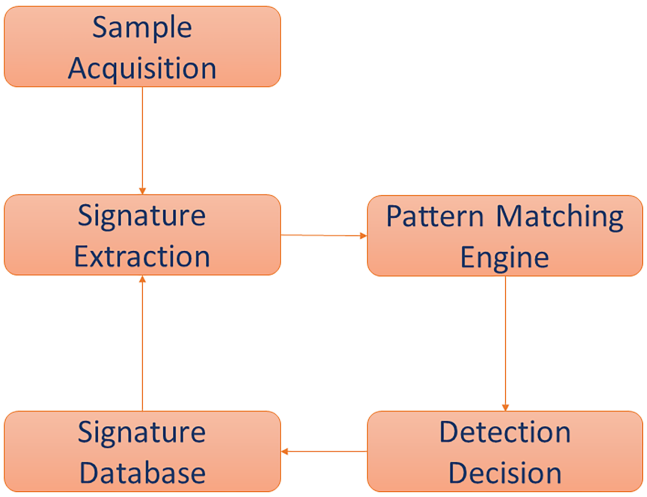

Figure 7: Signature base malware detection flow diagram

Recent research has focused on overcoming these limitations by integrating signature-based methods with advanced technologies and complementary strategies. Botacin et al. introduced *HEAVEN*, a hardware-enhanced antivirus engine designed to accelerate signature matching, demonstrating that dedicated hardware can substantially improve detection speed and throughput in large-scale environments [64]. Similarly, Selvaraj et al. compares a detection framework that leverages low-level system interactions to improve classification accuracy while reducing computational overhead [73]. Ojugo and Eboka employed an approximate Boyer–Moore algorithm to enhance signature matching efficiency [83], while Joe and Kim developed a greedy algorithm based on association analysis to streamline signature generation [33].

Pang et al. further improved detection performance through a random oversampling technique that balances imbalanced datasets and reduces classification bias [34].

Beyond speed and efficiency, researchers have sought to increase the adaptability and resilience of signature-based paradigm by combining them with complementary detection paradigms. Goyal and Kumar proposed a pipeline that integrates signature-based and behavior-based techniques, creating a more comprehensive defense capable of detecting both known and previously unseen malware [32]. Kwon et al. adopted a similar hybrid perspective, employing a statistical analysis unit to filter anomalies before using a Composite AutoEncoder (CAE) to reduce false negatives [77]. Al-Asli and Ghaleb provided a comparative analysis of static, dynamic, and hybrid detection strategies, emphasizing that specific design choices can significantly affect detection performance depending on the deployment context [35]. Kamdan et al. [122] investigated static malware detection using machine learning models, specifically focusing on Random Forest for classifying malicious software. It compared the performance of different machine learning algorithms in the static analysis domain.

A key area of advancement involves augmenting traditional signature-based systems with machine learning and data-driven techniques. Chakravarty et al. explored the integration of ML algorithms with signature-based detection to improve adaptability and classification accuracy [85], while Tirumala et al. utilized autoencoders to optimize training processes and enhance feature extraction from signature datasets [37]. Assegie introduced an optimized K-Nearest Neighbors (KNN) classifier, demonstrating how classical machine learning models can refine detection decisions based on signature characteristics [82]. Nahmias et al. extended this paradigm with *TrustSign*, which leverages deep feature transfer learning in private cloud environments to generate trusted signature sets [36]. Similarly, Shi et al. proposed *NBP-MS*, a network-behavior-profiling-based method that dynamically updates signatures based on observed activity, addressing the challenge of rapidly evolving threats [38]. Udayakumar et al. also advanced dynamic signature generation by tracking Application Programming Interface (API) calls during execution, enabling detection mechanisms to evolve in response to malware behavior [84].

Beyond traditional software-based detection, several studies have demonstrated that signature-based principles can be extended to specialized environments. Fouad and Abdel-Hamid applied Hidden Markov Models (HMM) to power consumption signatures for anomaly detection in IoT devices, illustrating the versatility of this technique in resource-constrained contexts [86]. Sihag et al. focused on Android malware, proposing a dynamic analysis approach that leverages kernel-level system logs for signature extraction and improved detection accuracy [74].

Overall, while signature-based detection continues to offer unmatched precision against known threats, its reactive nature limits its effectiveness against novel, obfuscated, and rapidly evolving malware. The trajectory of recent research indicates a shift toward hybrid systems that combine signature matching with behavioral analysis, machine learning, and hardware acceleration. Such approaches aim to transform signature-based detection from a static, pattern-matching tool into a dynamic, adaptive component within a multi-layered cybersecurity architecture. By incorporating automated signature generation, behavioral context, and intelligent feature extraction, future systems are poised to retain the strengths of signature-based detection while overcoming its traditional limitations. Nevertheless, the reactive nature of signature-based detection and its limited effectiveness against unknown or obfuscated malware necessitate complementary strategies. This limitation has driven the evolution of heuristic-based procedures, which aim to expand detection capabilities beyond known signatures by inferring malicious intent from behavioral characteristics.

4.2 Heuristic-Based Techniques

Building on the limitations of static signature matching, heuristic-based detection introduces greater adaptability by focusing on suspicious behaviors and program characteristics rather than predefined patterns. This shift allows security systems to recognize novel and previously unseen threats that would evade traditional signature databases. Unlike static signature matching, heuristic methods analyze behavioral traits, execution patterns, structural anomalies, and contextual indicators to infer malicious intent even when explicit signatures are unavailable. Flow of heuristic based techniques is depicted in Fig. 8. This makes heuristic analysis especially valuable in combating zero-day malware, polymorphic threats, and advanced evasion techniques that dynamically alter code to bypass conventional detection systems. Despite these advantages, heuristic models face persistent challenges, such as high false-positive rates, increased computational demands, and the complexity of accurately modeling evolving malware behavior. Recent research has sought to refine and extend heuristic detection capabilities through both algorithmic innovation and hybridization with other detection paradigms. Čisar and Joksimovic demonstrated how heuristic scanning combined with sandboxing significantly improves malware detection by isolating suspicious programs in controlled environments for detailed behavioral analysis [87]. This strategy allows analysts to observe execution characteristics without risking system integrity. Similarly, Alkhateeb and Stamp proposed a dynamic heuristic detection method leveraging a Naive Bayes classifier to identify packed malware by modeling behavioral deviations, thereby improving sensitivity to obfuscated threats [41]. Addressing the challenge of fileless malware—known for its ability to operate exclusively in memory and evade disk-based detection—Afreen et al. highlighted the importance of heuristic approaches that emphasize runtime analysis and memory inspection to identify such elusive attacks [40].

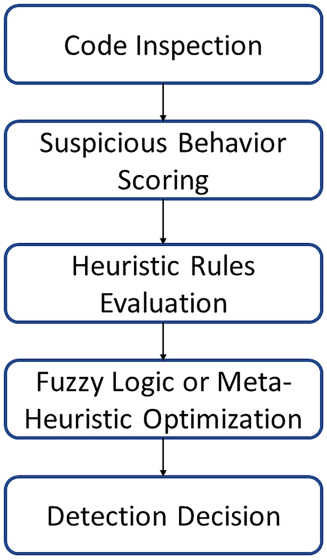

Figure 8: Heuristic base malware detection flow diagram

The integration of heuristic techniques with machine learning and meta-heuristic optimization has further enhanced detection accuracy and adaptability. Sharma and Agrawal introduced MH-DLdroid, a hybrid framework that combines meta-heuristic algorithms with deep learning models to improve Android malware detection, demonstrating significant gains in classification performance over traditional concepts [88]. Jhansi et al. proposed a two-tier detection framework that fuses fuzzy logic with meta-heuristics, resulting in a system capable of dynamically adapting its decision boundaries to evolving malware patterns [89]. Bhuiyan

et al. also explored multimodal feature selection strategies, showing that selecting low-correlated modalities significantly boosts the predictive performance of heuristic systems [94]. Likewise, Samarthrao designed a multi-objective feature selection mechanism combined with adaptive capsule networks for email spam detection, highlighting the growing convergence of heuristic analysis with deep learning architectures [93].

A complementary strand of research has focused on specialized heuristic rules and algorithmic enhancements aimed at improving detection coverage. Almeida and Westphall applied heuristic web scraping and crawling techniques to detect phishing URLs, demonstrating the utility of heuristic approaches in web-based threat scenarios [42]. Raja et al. developed MUDHR, a heuristic rule set for malicious URL detection, which substantially enhanced accuracy by leveraging structural and lexical features of URLs [92]. Arora et al. proposed a platform-independent Python-based tool, *ducky-detector*, which uses heuristic rules to identify malicious activities linked to USB Rubber Ducky devices, highlighting the adaptability of heuristic detection in hardware exploitation contexts [45]. Similarly, Dou et al. improved the traditional N-gram algorithm to enhance heuristic detection of unknown malware, increasing sensitivity to subtle code variations indicative of malicious intent [44]. Hajmasan et al. explored the use of bytecode-level heuristic signatures, demonstrating that program-level instruction patterns can effectively reveal behavioral anomalies [91].

Other works have expanded the scope of heuristic analysis by exploring execution-level and system interaction patterns. Suryati and Budiono proposed a detection framework based on API call network analysis, enabling systems to identify suspicious behaviors based on deviations in API interaction graphs [90]. Odat and Yaseen leveraged the co-occurrence of multiple feature sets within malware samples to improve detection precision, illustrating the value of feature interactions in heuristic classification [39]. Chavan et al. implemented a hybrid antivirus system that integrates heuristic rules with signature databases, demonstrating that combining static and behavioral indicators significantly improves detection coverage, particularly on portable devices [43].

The breadth of these studies reflects a broader trend: heuristic detection is transitioning from a rule-based supplementary technique to a central component of modern, adaptive cybersecurity architectures. While false positives and computational overhead remain critical concerns, the fusion of heuristic analysis with machine learning, fuzzy logic, and feature engineering has dramatically improved detection precision and resilience. Furthermore, heuristic methods excel in domains where behavioral context, environmental interactions, or runtime characteristics offer more reliable indicators of malicious activity than static signatures. Future directions are likely to focus on optimizing heuristic models for real-time deployment, integrating them with explainable AI (XAI) to enhance interpretability, and developing adaptive heuristics capable of evolving alongside the threats they are designed to detect.

4.3 Behavior-Based Techniques

Extending beyond heuristic inference, behavioral-based detection emphasizes direct observation of program actions and system interactions, providing richer contextual signals for identifying malicious activity. Behavioral-based malware detection represents one of the most dynamic and adaptive strategy in contemporary cybersecurity, shifting the detection paradigm from static signatures and predefined patterns to the observation and analysis of program actions in real time. Instead of matching known code fragments, these techniques monitor behavioral indicators, such as anomalous file modifications, unauthorized network connections, suspicious memory usage, or unexpected access to system resources, to infer malicious intent. Flow of behavior based techniques is depicted in Fig. 9. This proactive nature enables the detection of previously unknown or rapidly evolving threats, including zero-day attacks and polymorphic malware, which often evade traditional signature-based defenses. However, the complexity of accurately modeling

and interpreting software behavior introduces significant challenges, such as elevated false-positive rates when benign applications exhibit unusual but legitimate activities, and increased computational overhead during continuous monitoring. Recent advancements in behavioral detection have sought to overcome these challenges by integrating graph-based modeling, semantic analysis, and machine learning to improve precision and interpretability. Fan et al. proposed a framework based on weighted heterography that captures and models relationships between malware features as graph structures, significantly enhancing classification performance [68]. Zhang et al. advanced this idea by focusing on method-level behavioral semantics, enabling their system to detect malicious patterns in Android applications by examining the contextual meaning of API usage [46]. Similarly, Xu et al. leveraged graph convolutional networks (GCNs) to analyze dependencies among behavioral features, demonstrating improved detection accuracy for complex malware families in Android environments [96]. In parallel, Anisetti et al. designed a lightweight detection system that collects multi-valued time series data within sandboxed environments to identify suspicious activity with minimal computational costs, making it suitable for deployment in resource-constrained systems [75].

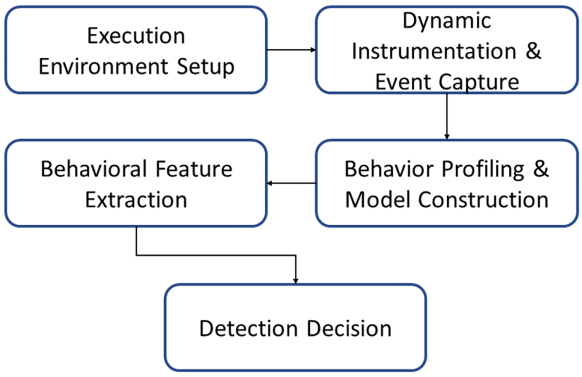

Figure 9: Behavior base malware detection flow diagram

The integration of deep learning with behavioral analysis has emerged as a powerful technique for capturing complex activity patterns and temporal dynamics [123]. Lu et al. introduced a hybrid deep learning model that combines convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to detect Android malware based on sequential behavior [95]. Abderrahmane et al. adopted a similar deep learning approach, utilizing CNNs to analyze system call sequences and accurately classify applications as benign or malicious [48]. Shakya and Dave also focused on system call analysis, demonstrating that patterns of low-level interactions can serve as highly discriminative features for malware classification [98]. Complementary to this, Singh and Singh applied traditional machine learning algorithms to behavioral artifacts, highlighting the ongoing relevance of non-deep learning methods when carefully tuned to behavioral indicators [99].

The versatility of behavioral-based detection is further evidenced by its adaptation to diverse threat landscapes and specialized environments. Sihwail et al. proposed a memory analysis-based approach that identifies malware based on in-memory behaviors, addressing the limitations of disk-centric methods [111]. Aslan et al. extended behavioral analysis to cloud environments, developing an intelligent detection framework capable of handling the unique challenges of virtualized infrastructures [49]. Sun et al. tackled Industrial Internet of Things (IIoT) scenarios by employing classified behavioral graphs to detect malicious activity within resource-constrained networks [100]. Similarly, Du et al. utilized classified behavior patterns to identify malware variants, illustrating how behavioral profiling can aid in family-level classification and lineage tracking [50]. Rosli et al. proposed a clustering-based model to group malware according

to behavioral similarities, enabling improved understanding of malware ecosystems and facilitating the identification of new threat families [101]. Hossain et al. have highlighted threshold-specific performance, showing that Bi-GRU excels at lower thresholds, while GRU performs optimally at higher thresholds, showcasing adaptability to varying configurations demonstrated by enhancing the performance of traditional models such as Naive Bayes and XGBoost, surpassing Gradient Boosting [124]. Kumar et al. emphasized the importance of early-stage behavior analysis, proposing a detection framework that monitors initial execution traces to rapidly classify malicious activity before significant damage occurs [102].

Behavioral strategies have also been successfully applied to domain-specific challenges. Muhtadi and Almaarif examined the influence of malware on network traffic, demonstrating the effectiveness of behavioral detection in capturing subtle anomalies that traditional packet inspection might overlook [97]. Tanana and Tanana addressed the rising threat of cryptojacking malware, emphasizing the role of behavioral indicators—such as abnormal resource consumption—in detecting mining activities [47]. These studies collectively underscore the adaptability of behavioral techniques across a spectrum of threat types and operating contexts.

4.4 Machine Learning-Based Techniques

Machine learning (ML)-based malware detection has emerged as one of the most transformative approaches in modern cybersecurity, enabling systems to automatically learn complex malicious patterns from data and continuously adapt to evolving threats. Unlike traditional static or heuristic techniques, ML-based systems are capable of discovering subtle, non-linear relationships between features, behaviors, and network activities that may not be explicitly defined by human experts [125]. By leveraging large datasets and advanced learning algorithms, these models can detect anomalies, classify new malware variants, and even predict emerging threats in real time. Their ability to self-improve as new data becomes available makes ML an indispensable tool in the arms race against increasingly sophisticated cyberattacks. However, challenges remain, including the need for high-quality labeled datasets, model interpretability, resistance to adversarial manipulation, and computational efficiency especially in resource-constrained environments such as IoT and mobile platforms [113,126].

Early works in ML-based detection explored traditional classification algorithms to detect malicious behaviors from software activity patterns. Singh and Singh applied machine learning techniques within the Cuckoo Sandbox environment to identify malicious artifacts based on behavioral indicators, demonstrating how automated feature extraction can significantly improve detection accuracy [99]. Khammas focused on improving ransomware detection using the Random Forest algorithm, which achieved notable success in classifying ransomware based on behavioral signatures and system-level events [103]. Similarly, Jang and Lee targeted intranet attacks by applying ML algorithms to network traffic data, revealing the potential of behavioral modeling in detecting insider threats and lateral movement [51]. Bae et al. further compared the performance of various machine learning models on ransomware detection, concluding that a combination of behavioral and static features yields the highest detection accuracy [107]. Complementing this, Kumari and Mrunalini used ML classifiers to detect denial-of-service (DoS) attacks, emphasizing the versatility of machine learning across different threat categories [105]. He et al. introduced AdvDroidZero, an efficient query-based attack framework against ML-based AMD methods that operates under the zero knowledge setting [72].

Deep learning has further advanced malware detection by automatically learning hierarchical feature representations from raw data, eliminating the need for extensive manual feature engineering. Fallah and Bidgoly designed a two-layer deep learning architecture that analyzes network traffic to identify malicious behavior patterns, significantly improving detection precision [104]. Ajvad Haneef and Madhu kumar

applied deep neural networks (DNNs) to detect metamorphic malware, showcasing how deep architectures excel at capturing subtle code transformations that evade traditional methods [58]. Vinayakumar et al. proposed robust malware detection models using deep learning, highlighting their superior generalization capabilities compared to shallow algorithms [57]. Hwang et al. also introduced a two-stage ransomware detection framework combining dynamic analysis with ML classifiers, improving detection at both early and late attack phases [106]. Odat and Yaseen leveraged feature co-existence patterns to design a novel Android malware detection model, illustrating the importance of feature engineering in improving classifier performance [39].

Specialized ML applications have also emerged in detecting malware within specific domains and threat vectors. Ibrahim et al. proposed a multilayered ML framework for botnet detection, combining filtering and classification modules to effectively identify command-and-control server communication [53]. Ali et al. extended this concept by employing a model stacking approach, where outputs from multiple deep learning models including Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN) are fused to improve detection accuracy in IoT environments [54]. Hussain et al. focused on early-stage prevention by detecting botnet scanning activity before an attack progresses, highlighting how ML can be leveraged for proactive defense [55]. Usman et al. used ML to analyze IP reputation data for dynamic malware detection, demonstrating its utility in forensic investigations and network-level security [65]. Feng et al. optimized deep learning models for mobile platforms by designing lightweight architectures that maintain a balance between accuracy and computational cost, making ML-based detection feasible for resource-limited devices [52]. An et al. presented a dual Siamese network-based detection system that uses byte pictures transformed from malware binary data to grayscale and opcode frequency-based images obtained after extracting opcodes and translating them into 2-gram frequencies [79]. Kil et al. offer a memory-efficient intrusion detection system that employs multi-binary classifiers and optimal feature selection. The proposed approach detects many forms of harmful attacks using parallel binary classifiers and optimal features for each attack type [80]. Chang discussed static analysis and malware detection using machine learning models, leveraging PE-header features and a stacking ensemble method. The research shows how combining different ML models can improve the performance of malware detection systems [127]. Akhtar and Feng valuated various machine learning algorithms for malware detection and classification, offering insights into their effectiveness in identifying malicious software. It compared traditional ML techniques like Random Forest with newer models to determine the best approach for malware classification [128].

Beyond traditional numerical features, vision-based approaches have gained traction as innovative alternatives to conventional detection pipelines. Roseline et al. explored deep random forest models applied to image representations of malware, where visual artifacts serve as discriminative features for classification [56]. This vision-based perspective aligns with broader trends toward multimodal malware detection, where data from diverse domains is fused for improved detection outcomes including system logs, network traffic, and visual patterns. Bensaoud et al. and Song et al. presented a comprehensive survey on the use of deep learning techniques for malware detection, highlighting the most effective models and methodologies [23,31]. Pathak et al. explored a machine learning approach for detecting Android malware using permission-based feature selection. It demonstrated how feature extraction based on app permissions can enhance the detection of malicious Android apps [129]. Ali et al. provided comprehensive review of learning techniques used for malware detection in IoT environments, emphasizing the challenges and solutions tailored for IoT security. It discussed various machine learning and deep learning techniques applicable to the unique needs of IoT devices [130]. Gorment and Krejcar offered a taxonomy of machine learning algorithms for malware detection, covering the current challenges and future directions in the

field. It served as a guide for researchers and practitioners in selecting appropriate machine learning models for malware classification [131]. Kumar & Sachan introduced an automated machine learning (AutoML) framework for malware detection, aiming to streamline model selection and hyperparameter tuning. It discussed the potential benefits of AutoML in cybersecurity for faster and more efficient malware detection systems [132]. Ali et al. examined the use of machine learning for malware detection in Internet of Things (IoT) environments, detailing the challenges and opportunities in this rapidly growing field. The authors focused on how to effectively apply ML techniques to secure IoT systems from malware attacks [130]. Al-Ghanem et al. proposed a novel approach to malware detection using attention-based deep convolutional neural networks (CNNs). The method is designed to improve the accuracy and efficiency of detecting malware by focusing on critical features using an attention mechanism [81].

Overall, ML-based malware detection has matured into a cornerstone of intelligent cybersecurity systems, offering scalability, adaptability, and predictive capabilities unmatched by traditional methods. Despite these strengths, challenges persist particularly in explainability, robustness against adversarial attacks, and the need for extensive labeled datasets. Current research trends increasingly emphasize hybrid models that combine multiple ML algorithms, lightweight architectures for edge environments, and the integration of behavioral, network, and visual features into unified detection frameworks. Such advancements are shaping the future of malware detection toward systems that are not only accurate and adaptive but also resilient and transparent in the face of evolving cyber threats. The classification algorithms employed across various ML-based malware detection approaches are summarized in Fig. 10, illustrating the diversity of machine learning techniques utilized for threat identification and analysis.

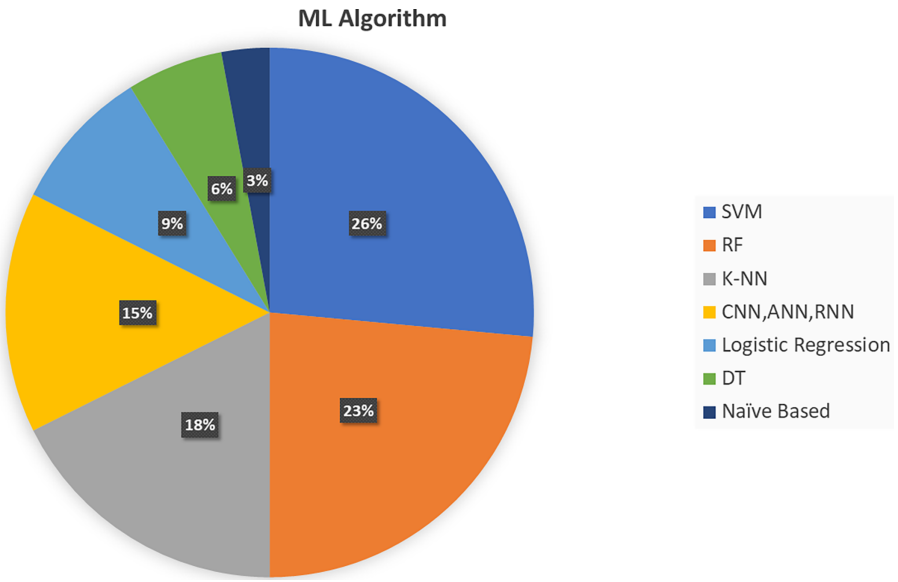

Figure 10: ML algorithms used in malware detection

4.4.1 Feature Selection in Malware Detection

Feature selection plays a critical role in improving the accuracy, efficiency, and interpretability of machine learning models used for malware detection. Due to the high-dimensional nature of malware datasets,reducing the feature space without losing discriminative power is essential.

Feature selection methods can be broadly classified into three categories:

- **Filter methods**, such as Chi-square test, Information Gain, and Mutual Information, evaluate the relevance of each feature independently of the learning algorithm.
- **Wrapper methods**, like Recursive Feature Elimination (RFE), evaluate subsets of features based on model performance, albeit with higher computational cost.
- **Embedded methods**, such as Lasso regression and feature importance scores from Random Forests, perform selection during model training.

In malware detection literature, feature selection has been used to reduce overfitting and improve detection speed. For example, Bhuiyan et al. [94] demonstrated that selecting low-correlated modalities in multimodal ML models improved classification performance. Similarly, Raja et al. [92] used heuristic rules to select features from URLs, enhancing detection of phishing attempts. Furthermore, feature selection enhances the interpretability of detection models which is a critical aspect for building explainable AI (XAI) systems. By focusing on a smaller set of high-impact features, cybersecurity analysts can better understand why a particular sample was classified as malicious [70,78].

4.5 Image-Based Techniques

Image-based malware detection first proposed by Nataraj et al. [71], is a promising cybersecurity approach that identifies subtle changes in malware code and detects both packed and obfuscated malware [69]. This method involves converting malware binaries or behavioral logs into visual representations (image space), allowing for the visualization of underlying patterns and structures [133,134]. Subsequently, images are processed using deep learning techniques to detect malicious behaviors [135]. Traditional signature-based methods often struggle with obfuscated or polymorphic malware [73]; however, image-based techniques can effectively identify such threats by analysing visual patterns, even when malware has been altered to evade detection. Moreover, combining DL, which excels in pattern recognition, with anomaly detection can significantly improve malware detection. Liu et al. [59] utilized a Gray Level Co-occurrence Matrix (GLCM) and CNN in multi-class malware detection. Kwan [60] generated Markov images based on byte-level transfer frequencies, capturing global statistical properties of malware and enhancing them through normalization and histogram equalization for better performance. Prabhpreet Singh et al. have proposed a novel method for categorizing malware executables based on their visual representation by converting the malware binaries to grayscale images and then classifying them using CNN [136]. Pinhero et al. [66] utilized grayscale, RGB, and Markov images, along with Gabor filters, and fine-tuned CNN on the Malimg and Microsoft BIG2015 datasets with varying image dimensions, Fig. 11 illustrate its different depictions. Saridou et al. [108] applied α-cuts as a defuzzification to achieve sparse representations and integrated with CNN. In [109], the authors proposed a multifaceted detection approach employing a time-series-to-image conversion with clustering, probabilistic analysis, and CNN. Additionally, it integrates security principles of authentication, authorization, and accounting (AAA), enhancing system reliability. Baptista et al. [61] utilise Hilbert curves and a Self-Organizing Incremental Network (SOINN) to identify malware code in IoT. However, the method's efficacy is questioned on larger, more diverse datasets. Tekerek and Yapici [67] utilized the B2IMG algorithm for visualization and CycleGAN to rectify imbalanced data sizes among malware families, achieving accuracies of 99.86% and 99.60% on the BIG2015 and DumpWare10 datasets, respectively. The work [110] employed color image visualization and a deep convolutional neural network (DCNN) for the Industrial Internet of Things (IIoT) and achieved an accuracy of 97.81% on the IIoT dataset and 98.47% on the Windows dataset. Table 4 provides an overview of image-based methods, highlighting their applicability in various environments and diverse contexts.

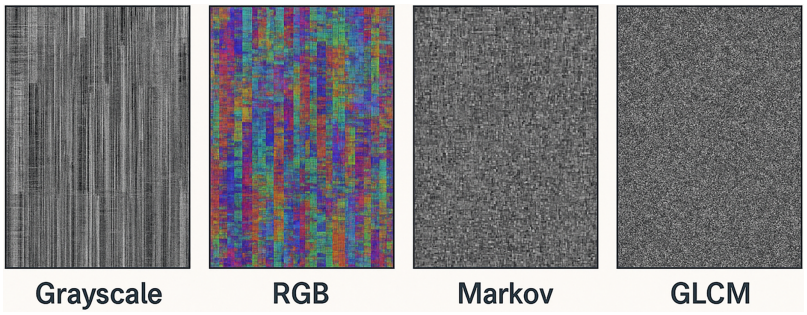

Figure 11: Malware representation in different formats

Table 4: Comparative overview of image-based malware detection methods

Author	Technique/Model	Accuracy/Performance	Strength	Limitation
Liu et al. [59]	GLCM + CNN	More than 90%	Good pattern capture	Limited scalability
Kwan [60]	Markov image generation + VGG19	97.3%	High accuracy	Potential parameter instability
Pinhero et al. [66]	Grayscale + RGB/Markov+ Gabor+ CNN	99.97% (Malimg)	High accuracy, low loss	Complexity, limited dataset specificity
Saridou et al. [108]	cf-cuts + CNN	93.60%	Dynamic flow representation	Requires complex computation
Ghahramani et al. [109]	Time series to image + AAA + CNN	Not explicitly stated	Integrated security principles	Lack of direct accuracy comparison
Baptista et al. [61]	Hilbert curves + SOINN	91.7%–94.1%	Good for IoT malware	Uncertain scalability to larger datasets
Tekerek and Yapici [67]	B2IMG + CycleGAN	99.69%–99.96%	Handles imbalanced data	Adversarial robustness unknown
Naeem et al. [110]	Color image visualization + DCNN	97.81%–98.47%	Good for IoT contexts	Needs additional analysis
Dharmalaksana et al. [62]	B2IMG + CNN + Gabor Filter	99.86%	Robust feature capture	Unknown adversarial robustness

To provide a holistic understanding of how different malware detection approaches compare across critical dimensions, Table 5 synthesizes their core strengths, limitations, and emerging research trends.The comparative overview underscores an ongoing paradigm shift toward hybrid and multimodal strategies that combine the strengths of multiple approaches to deliver more robust, scalable, and interpretable malware detection solutions.

Table 5: Comparative overview of malware detection approaches

Approach	Strengths	Limitations	Emerging trend
Signature-based	Fast, low false positives	Ineffective against zero-day malware	Integration with ML and hardware acceleration
Heuristic-based	Detects unknown threats	High false positive rate	Meta-heuristics and fuzzy logic for improved detection
Behavioral-based	Context-aware and effective against evolving threats	Resource-intensive and prone to false positives	Graph-based behavioral modeling
ML-based	Adaptive, scalable, and improves with data	Requires large datasets, limited interpretability	Explainable AI (XAI) and adversarial training
Image-based	Resistant to obfuscation and polymorphism	Computationally expensive	CycleGAN and multimodal fusion approaches

5 Critical Analysis of Datasets

Malware datasets play an important role in developing machine learning-based malware detection systems. They serve as foundational pillars of cybersecurity research and provide the raw material to analyze, detect, and combat evolving digital threats. Well-known datasets like VirusTotal, VirusShare, Malimg, Drebin, and CICIDS2017 provide insights into different aspects of malware behavior, aiding in the continuous improvement of cybersecurity solutions. However, their utilization comes with several challenges. One of the primary issues is data diversity and representativeness. Many datasets are biased toward specific malware families, attack types, or operating systems, making them less effective for real-world detection models. Additionally, malware evolves rapidly, and outdated datasets may not reflect the latest attack patterns, reducing their generalizability.

Another significant challenge for malware datasets is labeling quality and ground truth validation. Datasets like VirusTotal aggregate multiple antivirus results, these labels can sometimes be inconsistent, leading to misclassification. The reliability of ground truth is critical in training machine learning models, and errors in labeling can significantly impact performance. Access restrictions and legal concerns are also areas of concern, such as VirusTotal and VirusShare are high quality datasets but require special access permissions, which makes them less accessible to independent researchers. Handling and sharing malware datasets also involve legal and ethical considerations, as improper handling can lead to unintended security risks.

From a technical perspective, working with large-scale datasets demands substantial computational resources. Processing raw malware binaries, network traffic logs, or behavioral traces requires advanced feature extraction techniques, which can be computationally expensive. Furthermore, some datasets are imbalanced, with an overwhelming number of benign samples compared to malware, which results in bias. Finally, dataset standardization and interoperability remain a challenge. Different datasets use varying formats, different labeling schemes, and their own collection methodologies, which makes it difficult to integrate multiple sources for comprehensive analysis. Cyber Security researchers often have to spend significant time preprocessing and normalizing that data before it's effective utilization.

Addressing these challenges is crucial for improving malware detection models and ensuring that cybersecurity solutions remain effective against evolving threats. Future research should focus on enhancing dataset diversity, improving labeling accuracy, promoting open-access repositories, and developing efficient preprocessing techniques to optimize dataset usability in real-world cybersecurity applications. Table 6 presents a critical analysis of some of the most commonly used malware detection datasets in this study.

Table 6: Comparative analysis of malware detection datasets

Dataset	Malware focus	Size	Access	Limitations
VirusTotal	General	Millions	Restricted	Commercial access, limited free API queries
VirusShare	General	40M+	Restricted	Requires membership, raw samples, No labels
Drebin	Android	179,000	Public	Focused on Android malware, good for ML research
Malimg	Windows	9342	Public	Useful for image-based ML techniques only
AMD	Android	24,500	Public	Good for ML-based analysis, diverse families, not updated
ArgusLab	Android	Varies	Public	Good for reverse engineering, only static Android Application Package (APK)
CIC-ANDMAL17	Android	426,000	Public	Good for network-based detection, small dataset size
FFRI	Windows	Not specified	Public	Focused on dynamic malware behavior, require licensing
CAIDA 2017	Botnets, DDoS, Network-based	Large scale	Public	Useful for network anomaly detection, needs additional preprocessing
CTU-13	Botnet	13	Public	Good for botnet detection, outdated
UNSW-NB15	Network-based	2M+	Public	Used for intrusion detection research, not for real word scenarios
CICIDS2017	Intrusion detection	3M+	Public	Simulated, Good benchmark for Intrusion Detection System (IDS) research

6 Findings

This section presents a consolidated synthesis of the literature reviewed, offering evidence-based answers to the research questions (RQs) and integrating broader trends observed across multiple domains of malware detection. Rather than summarizing prior sections, the findings distill core insights derived from 89 peer-reviewed articles and contextualize them within overarching themes such as adaptability, transparency, scalability, and dataset quality.

6.1 RQ1: What Emerging Trends Have Defined Malware Evolution in the Past Decade, and in What Ways Do They Challenge Existing Detection Approaches?

Malware has undergone a dramatic evolution, marked by increased complexity, polymorphism, and the adoption of artificial intelligence (AI) techniques by adversaries. The integration of AI into malware development allows these threats to adapt dynamically, evade traditional defenses, and exploit novel vulnerabilities. Emerging trends include:

- **Fileless malware** that operates entirely in memory, bypassing signature-based detection mechanisms. Afreen et al. emphasized the need for runtime behavior monitoring to counter such threats [40].
- **Hybrid malware** leveraging modular designs for payload delivery, complicating detection through multi-stage attacks.
- **Target-specific ransomware** utilizing advanced encryption and social engineering, now among the most disruptive forms of malware. Random Forest-based approaches have been proposed for its detection [103].
- **IoT and Industrial IoT (IIoT) exploitation**, due to weak device-level security. Sun et al. proposed behavior-graph-based models to secure IoT networks [100].
- **Advanced Persistent Threats (APTs)** backed by state actors pose long-term threats by maintaining persistent access to networks. Botacin et al. introduced hardware-enhanced AV systems for real-time APT detection [64].

6.2 RQ2: How Are Current Malware Detection Techniques Addressing Modern and Evasive Malware Threats?

Recent innovations have significantly enhanced the performance and scope of detection techniques:

- **Signature-based detection** has been refined with optimized algorithms. The Boyer-Moore algorithm [83] and K-Nearest Neighbors (KNN) [82] offer better speed and efficiency. However, these are still prone to evasion by new malware variants.
- **Heuristic and behavioral techniques** now incorporate ML-driven rule sets to capture unknown malware characteristics. For example, the use of Naive Bayes for packed malware detection offers higher sensitivity to obfuscation [41], while heuristic phishing detection improves malicious URL identification [42].
- **Hybrid frameworks** that combine signature-based and behavioral analysis—such as those proposed by Goyal and Kumar [32], and Chavan et al. [43]—have demonstrated superior accuracy in recognizing previously unseen malware.
- **Hardware-level detection systems** (e.g., HLMD [73]) and hybrid AV engines like HEAVEN [64] offer real-time responsiveness, showing the potential of integrated detection pipelines.
- **AI-based detection systems** are highly resilient. They learn, improve and adapt over time as they are exposed to more data. Combination of ML with deep learning can capture complex patterns in the data. ML-based methods are scalable and can be deployed across various environments. Accuracy measure of related research is depicted in graphical representation at Fig. 12. It shows that more than 90% of the proposed methods have efficacy rate above 90%. Image-based malware detection has also improved the ability to detect obfuscated malware. Studies in Table 4 show that these techniques are effective against modern malware with over 97% accuracy. These advancements highlight the growing potential of image-based methods to detect even complex and hidden malware.

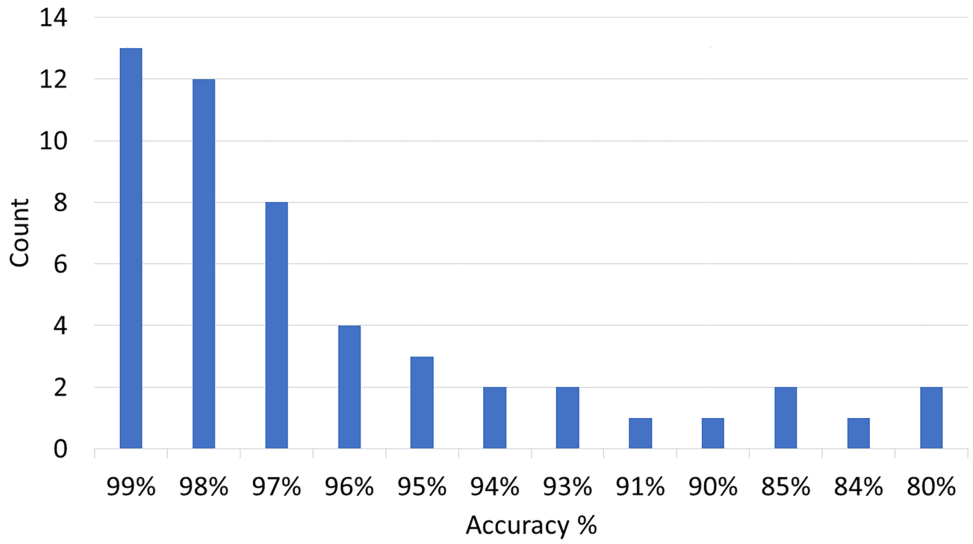

Figure 12: Accuracy of malware detection techniques reported in reviewed papers

Overall, these advancements shift malware detection from static signature-matching to dynamic, context-aware, and adaptive systems that leverage multiple data modalities.

6.3 RQ3: In What Ways Do Malware Dataset Characteristics Influence the Reproducibility and Reliability of Detection Models?

The performance and reliability of AI/ML-based malware detectors are tightly coupled with the quality and diversity of training datasets. The review identifies several widely used datasets:

- **VirusTotal** and **VirusShare** offer large malware repositories but have access constraints or lack metadata labeling.
- **Drebin**, **AMD**, and **CIC-ANDMAL17** support Android-focused detection models.
- **Malimg** and **FFRI** cater to image-based and dynamic behavior analysis, respectively.
- **UNSW-NB15** and **CICIDS2017** are valuable for detecting network intrusions and DoS attacks.

However, common limitations include:

- Data imbalance and class sparsity.
- Outdated samples that don't reflect recent threat evolution.
- Lack of behavioral metadata, such as API traces or system-call patterns.

High-quality datasets like the ones used by Udayakumar et al. [84] include API traces and early-stage malware execution data are essential for enhancing generalizability and early detection capabilities. A comprehensive overview of the datasets and sources commonly employed in recent malware detection literature is presented in Table 7. This table highlights the frequency and context in which each dataset has been utilized across various studies, providing insight into prevailing research trends, preferred data modalities, and the alignment of specific datasets with different detection objectives. By systematically mapping these references, the table serves as a valuable resource for identifying dataset popularity and opportunities for future dataset enhancements.

Table 7: Overview of datasets, counts, and corresponding references

Dataset	Usage (Count)	References
VirusTotal	8	[11,32,41,68,75,99,103,104]
VirusShare	7	[12,34,43,44,95,99,106]
Drebin	5	[12,39,46,52,96]
Malimg	3	[56–58]
CICIDS2017	2	[51,55]
CTU-13	2	[38,53]
CIC-ANDMAL2017	2	[98,104]
AMD	1	[46]
ArgusLab	1	[48]
FFRI	1	[107]
CAIDA 2017	1	[105]
UNSW-NB15	1	[54]

6.4 RQ4: How Can AI-Driven Cybersecurity Solutions Be Applied to Improve the Scalability and Efficiency of Malware Detection Systems?

AI-driven solutions have redefined the capabilities of modern cybersecurity systems:

- **Deep learning models**, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, extract intricate patterns from raw malware binaries and network traffic, offering state-of-the-art accuracy rates exceeding 90% across most benchmark datasets (see Fig. 13).
- **Explainable AI (XAI)** is being gradually introduced to improve model transparency and interpretability, although its adoption in malware detection remains limited.
- **Real-time inference and adaptive learning** enable AI systems to respond instantly to zero-day threats. The TrustSign model [36] and the adaptive heuristics proposed by Shakya and Dave [98] are prime examples of this advancement.
- **Scalability** is achieved through federated learning and distributed detection architectures that minimize reliance on central resources. Vision-based models further extend AI utility by transforming malware binaries into grayscale images for visual feature extraction, often achieving over 97% detection accuracy using techniques such as GLCM and CycleGAN [63,67].

Despite these benefits, challenges such as adversarial evasion, data poisoning, and lack of interpretability must be addressed through hybrid AI frameworks and privacy-preserving solutions.

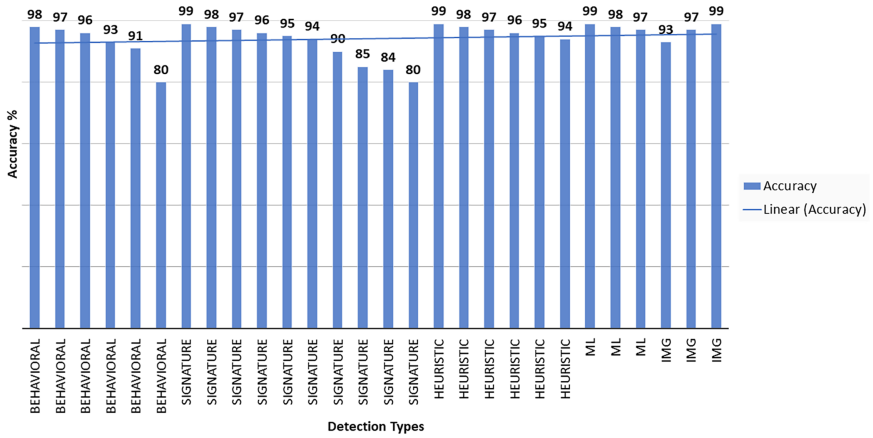

Figure 13: Comparison of accuracy across different malware detection techniques

7 Discussions

This section contains a discussion of outcomes obtained from this survey. The shortcomings and problems of existing systems are addressed. A model is proposed as a guideline for practitioners and academics in designing malware detection applications and implications are also offered as future directions of the underlying area.

7.1 Conceptual Framework

An integrated analytical framework resulting from the theme synthesis of all 89 analyzed research is presented in Fig. 14. Instead of being a purely conceptual model, this framework was inductively constructed from recurring methodological patterns identified across high-quality studies (QEI greater than equal to 7). It demonstrates how different detection paradigms—static, dynamic, hybrid, and image-based—interact and complement each other to form a comprehensive malware detection pipeline.

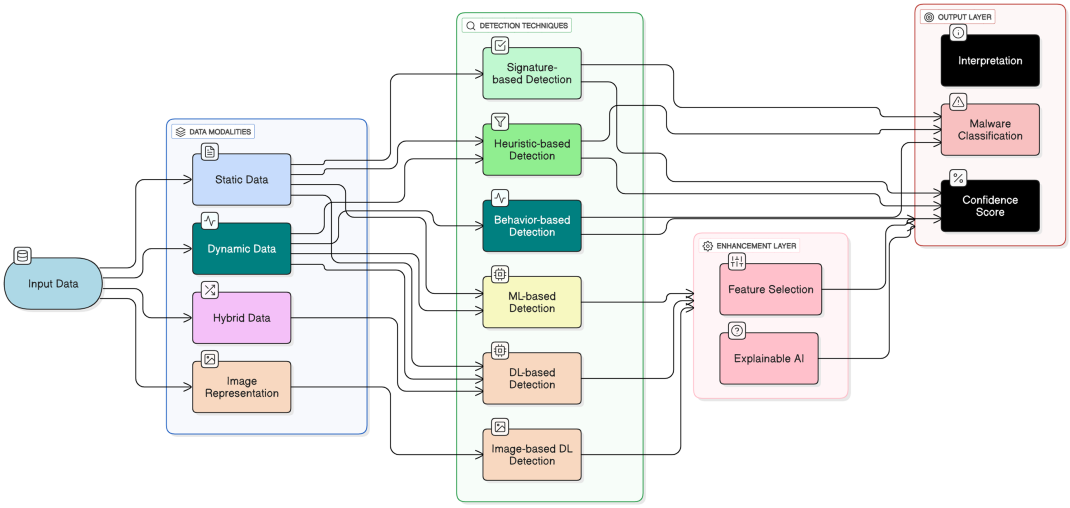

Figure 14: A conceptual framework illustrating the layered process of malware detection using diverse input modalities and detection techniques

The framework begins with multiple sources of data, including static code features, runtime behaviors, hybrid datasets, and image-based representations of malware samples. These data types correspond to a range of detection approaches, from traditional signature and heuristic analysis to advanced machine learning and deep learning methods. Intelligent models are further refined through effective feature selection, enabling them to concentrate on the most discriminative characteristics of malicious activity. In cases where malware is represented as images, deep learning architectures can capture subtle structural and texture-based patterns that conventional methods may overlook. To ensure that automated decisions remain interpretable and trustworthy, the framework incorporates explainable AI (XAI) techniques such as SHapley Additive exPlanations (SHAP), Local Interpretable Model-agnostic Explanations (LIME), and radient-weighted Class Activation Mapping (Grad-CAM). These tools help clarify how models reach their conclusions, providing analysts with transparent and actionable explanations.

The final outcome is a clear and supported judgment along with a reason for that decision. Overall, this framework helps security professionals and researchers better understand how different techniques and tools can be combined to improve malware detection and make the results more transparent and useful in real-world scenarios. Table 8 further illustrates the functional workflow of the proposed framework, detailing each component's role and its relevance to real-world deployment scenarios.

Table 8: Functional breakdown and real-world relevance of the proposed framework (Fig. 14)

Framework component	Primary function in detection pipeline	Real-world application/Benefit
Data acquisition & Preprocessing	Collects malware and benign samples from multiple sources (e.g., EMBER, CIC-MalMem2022) and performs cleaning, normalization, and feature extraction.	Ensures standardized and high-quality input data, improving reproducibility and reducing bias in model training.
Feature engineering & Dimensionality reduction	Identifies the most discriminative features using techniques like PCA, mutual information, or evolutionary feature selection.	Reduces computational complexity and enhances model interpretability, especially on resource-constrained devices.
Model selection	Explores various ML/DL architectures (e.g., CNN, RNN, LSTM, hybrid models) and selects the best-performing model based on defined metrics.	Eliminates manual tuning effort and adapts detection strategy dynamically as malware evolves.
Explainable AI (XAI) module	Provides interpretable insights into classification decisions using methods like SHAP or LIME.	Enhances analyst trust, supports forensic investigations, and aids in compliance with regulatory requirements.

(Continued)

Table 8 (continued)

Framework component	Primary function in detection pipeline	Real-world application/Benefit
Adversarial robustness layer	Incorporates adversarial training and anomaly detection techniques to defend against evasion attacks and adversarial malware.	Improves model resilience against adaptive threats and unknown attack patterns.
Privacy-preserving layer	Employs techniques such as federated learning, differential privacy, or homomorphic encryption to safeguard sensitive data during model training.	Ensures secure collaborative learning across organizations without sharing raw data, aligning with General Data Protection Regulation (GDPR) and enterprise policies.
Deployment & Scalability module	Packages the final model into deployable containers for cloud, edge, or IoT devices, supporting real-time inference and updates.	Enables scalable and adaptive deployment in diverse environments (enterprise networks, IoT systems, SOC platforms).

7.2 Advice for the Practitioners

Practitioners can consider the following advice based on the insights gathered from the referenced literature on malware detection techniques. Practitioners can leverage hardware-accelerated solutions like HEAVEN to improve the performance of real-time, signature-based malware detection. By integrating hardware enhancements it becomes possible to accelerate detection processes and reduce the computational load on software-based systems [64]. Implementing advanced algorithms such as the approximate Boyer Moore algorithm, string matching can enhance signature-based detection by improving the speed and accuracy of pattern matching in malware signatures [83].

Utilizing machine learning models to assist in signature and heuristic-based detection can significantly improve malware detection rates on Android devices. These models can learn from vast datasets. It results in identifying subtle patterns that traditional methods might miss [36,57,58]. Optimizing K-Nearest Neighbors (KNN) models for signature-based detection can enhance the accuracy and efficiency of malware identification, particularly in diverse and evolving threat landscapes [36,57,58].

Implementing greedy algorithms for generating malware signatures can streamline the detection process by quickly identifying the most relevant patterns and reducing the time required for signature generation [42,91]. Combining heuristic methods with signature-based detection allows for a more flexible and adaptive approach to identify new and unknown malware based on behavior rather than predefined patterns [42,91].

Utilizing Hidden Markov Model (HMM) for detecting anomalies in IoT power signatures can provide an effective means of identifying malware based on deviations from normal power usage patterns [48,53]. Using auto-encoders for feature extraction in malware classification can help reduce the dimensionality of data and highlight the most relevant features for accurate and efficient detection [36,57,58].

Incorporating network behavior profiling into malware signature generation can provide a more holistic view of malware activity, improving detection rates by considering network-level behaviors [50,100]. Combining static signature-based detection with dynamic behavior-based methods can offer a more comprehensive intrusion detection system, capable of identifying both known and unknown threats [32,77,95].

7.3 Potential Use in Applications

Malware detection applications are the need of the hour to safeguard sensitive data and critical infrastructure from cyber threats. These tools play a vital role in identifying, preventing, and mitigating malicious software attacks that can compromise security and disrupt operations. Various sectors can greatly benefit from malware detection technologies.

i. **Cybersecurity in Enterprise Networks:** Advanced malware detection can be used in corporate environments to prevent cyberattacks on business-critical infrastructure. Endpoint security can be enhanced using ML/DL-based detection techniques.
ii. **Healthcare:** With the rise of digital health records and telemedicine, the healthcare sector is a prime target for cyberattacks. AI-based Malware detection techniques can help protect patient records, hospital networks, and medical devices from ransomware and data breaches.
iii. **Finance and Banking:** Banks and financial institutions are frequently targeted by hackers looking to steal customer information or disrupt financial transactions. Banking fraud, phishing attacks, and unauthorized access to accounts can be prevented leveraging ML/DL-based malware detection models.
iv. **Government and Defense:** Government agencies store highly sensitive national security data and citizen information, making them prime targets for cyber espionage and cyber warfare. Malware detection applications protect classified files, secure communication networks, and prevent foreign attacks.
v. **Education and Research Institutions:** Universities and research centers hold valuable intellectual property, research data, and personal information of students and faculty. Malware detection tools help secure these databases from cybercriminals and unauthorized access. Security solutions such as Sophos Intercept X, Bitdefender GravityZone, and ESET Endpoint Security are widely used in educational institutions.
vi. **Corporate and Business Sector:** Companies across industries require malware detection tools to protect sensitive business information, financial transactions, and employee data. These tools help prevent ransomware attacks, insider threats, and data leaks.

7.4 Limitations of This Study

While the referenced literature on malware detection techniques provides valuable insights, it's important to acknowledge certain limitations and challenges identified across the studies. The rapid evolution of malware means that findings can quickly become outdated. New types of malware and detection techniques may emerge after the publication of this research, necessitating continuous updates and follow-up studies. Datasets may not encompass the full range of malware types and variants. This can lead to models that perform well on the training data but fail to generalize to new, unseen malware. Often, datasets may lack detailed metadata about each sample, such as the method of delivery, behavior, and impact. This lack of context can hinder the development of comprehensive detection techniques. Some high-quality datasets may be proprietary or restricted, limiting access for researchers. This can impede the ability to benchmark and compare different detection methods.

Given the evolving nature of malware and the rapid advancement of technology, several future directions stand out as particularly important for improving detection systems. One such direction is federated learning, which allows models to be trained across different devices or organizations without

exposing sensitive data—offering both privacy and scalability. Similarly, privacy-preserving techniques, such as homomorphic encryption and differential privacy, are becoming essential, especially in fields like healthcare and finance where data confidentiality is paramount. Another area gaining traction is the creation of synthetic datasets using methods like Generative Adversarial Networks (GANs), which can help fill data gaps and make models more resilient. Self-supervised learning also shows promise, as it can make use of vast amounts of unlabeled malware data, reducing the need for time-consuming manual labeling. The integration of real-time threat intelligence into detection models can help systems adapt more quickly to new or unknown threats. Lastly, improving a model's ability to generalize across different environments and datasets is critical for ensuring reliable performance outside of controlled research settings. Exploring these avenues can help build more robust, adaptable, and trustworthy malware detection systems for the future.

By acknowledging these limitations, researchers and practitioners can steer future advancements in malware detection techniques, aiming to overcome these challenges and improve the overall effectiveness and sustainability of these technologies in practical malware detection applications.

7.5 Challenges and Future Work

Ensuring reliable real-time detection while maintaining system performance remains a persistent difficulty. Hardware-assisted solutions, such as the HEAVEN antivirus engine, demonstrate promise in accelerating malware analysis but still face inherent trade-offs between processing speed and computational overhead [64]. As the volume of malware and network traffic expands exponentially, scalability has become a critical bottleneck. Many existing frameworks struggle to efficiently process and analyze the vast, heterogeneous data produced by contemporary digital infrastructures [32]. Furthermore, it's a constant concern to strike a sustainable balance between false positives and false negatives because too many false positives might overwhelm analysts and false negatives let malicious behavior go undetected [84].

Detection challenges are further compounded in resource-constrained environments, particularly within IoT ecosystems, where devices often lack the computational capacity required for advanced analytical models [86]. Additionally, the proliferation of multimedia data spanning images, videos, and audio introduces new complexities for malware detection. The integration of IoT-driven, data-intensive applications for monitoring and control amplifies the exposure to sophisticated threats such as man-in-the-middle attacks [137] and large-scale botnets like Mirai, which can manipulate or disrupt critical multimedia streams [138]. These findings collectively emphasize that future research should prioritize lightweight, scalable, and adaptive detection models that can maintain performance and interpretability across diverse and resource-limited environments [139].

The future directions, illustrated in Table 9, lead to development of hybrid approaches that combine signature-based and behavior-based detection can enhance the effectiveness of malware detection. Such methods leverage the strengths of both techniques to improve accuracy and reduce false positives [33]. Integrating machine learning with signature and heuristic-based detection can further improve detection capabilities. Machine learning models can adapt to new malware variants and identify previously unknown threats [85,106].

Table 9: Future directions in malware detection with key focus areas

Direction	Focus area	Details
Development of hybrid approaches	Combination of Signature with behavior-based detection	Integrate machine learning
Deep learning techniques for malware detection	Use of CNN & Graph Convolutional Network (GCN)	Transfer learning to improve efficiency
Heuristic scanning and sandboxing	Controlled environment	Check actions, not just signatures
Encouraging cross-disciplinary research	Cybersecurity + data science + hardware	Collaborative development across domains
Real-time threat intelligence system	Automated threat feeds	Enhance responsiveness and adaptability
Privacy-preserving malware analysis	Use of encryption techniques	Enable secure processing of sensitive data
Interpretable machine learning models	Use of XAI	Improve explainability and trust

Employing deep learning techniques can enhance malware detection by identifying complex patterns in large datasets. Techniques such as convolutional neural networks (CNNs) and graph convolutional networks (GCNs) have shown promise in detecting malware based on behavior analysis [48,96]. Leveraging transfer learning can improve the efficiency of malware detection models by utilizing pre-trained models on related tasks, thereby reducing the need for extensive training data [36]. Utilizing heuristic scanning and sandboxing can detect malware by observing its behavior in a controlled environment. This method can identify previously unknown threats based on their actions rather than their signatures [87]. Encouraging cross-disciplinary research can lead to innovative solutions. Collaboration between cybersecurity experts, data scientists, and hardware engineers can result in more robust and efficient malware detection systems [64,140].

Developing systems that can automatically gather and analyze threat intelligence in real-time can enhance the speed and accuracy of malware detection. Integrating automated threat intelligence with detection systems can provide timely updates and responses to emerging threats [39]. Implementing privacy-preserving techniques for malware analysis can protect sensitive data while allowing effective threat detection. Techniques such as homomorphic encryption and multi-party secure computation can be explored [36]. Developing interpretable machine learning models for malware detection can improve trust and adoption. Explainable AI techniques can provide insights into the decision-making process of detection models, aiding cybersecurity analysts in understanding and responding to threats [55]. Additionally, addressing the growing challenge of adversarial attacks is critical, as attackers increasingly craft inputs designed to evade detection models [28]. Enhancing model robustness against such attacks—through adversarial training, detection of adversarial behavior, or robust feature selection should be prioritized in future research to maintain the reliability and security of AI-based detection systems.

One of the ongoing challenges in malware detection is the lack of diverse and high-quality datasets, primarily due to privacy constraints and restricted access to real-world malware samples. This limitation hampers the ability of detection models to generalize effectively. As a future direction, synthetic data

generation presents a promising solution by enabling the creation of artificial but representative malware samples or behaviors. Such data can be used to augment existing datasets without risking exposure to live threats [76].

While prior surveys have primarily emphasized accuracy and efficiency of malware detection models privacy and trustworthiness is an equally critical dimension which remains underexplored. The increasing reliance on centralized malware datasets poses privacy concerns, especially when training models on sensitive or proprietary data. Techniques such as *federated learning (FL)*, *homomorphic encryption (HE)*, and *differential privacy (DP)* are gaining traction as mechanisms to ensure that malware detection models can be trained collaboratively without exposing raw data. Similarly, the generation of synthetic malware samples using GANs and diffusion models has emerged as a means to supplement training datasets while safeguarding sensitive information.

In parallel, trustworthiness is closely tied to the explainability and robustness of AI-driven malware detectors. Recent studies have highlighted the vulnerability of deep learning models to adversarial manipulation, where minor perturbations in features can evade detection. The integration of *Explainable AI (XAI)* frameworks such as SHAP, LIME, and attention-based visualization can enhance analyst confidence by clarifying model decisions. Moreover, adversarial training and hybrid models offer pathways to strengthen resilience against evolving malware evasion strategies.

However, these privacy-preserving and trustworthy AI techniques often come at the cost of increased computational overhead, raising an important trade-off: *How can malware detection systems simultaneously achieve high accuracy, privacy preservation, scalability, and robustness in resource-constrained environments?* This trade-off underscores an open research challenge and highlights a unique contribution of this survey—drawing attention to the interplay between privacy, trustworthiness, and efficiency in next-generation malware detection.

We hope this survey study inspires further research in the field of malware detection. Future research opportunities abound, including exploring the distinctive features of various malware, developing advanced methods for identifying and investigating attacks, predicting malware behavior, extracting relevant features, and enhancing detection efficacy.

8 Conclusion

This review brings together recent developments in malware detection by examining traditional, heuristic, machine learning, and deep learning approaches, and comparing their respective strengths, limitations, and operational characteristics. By systematically analyzing these methods, the review offers a coherent perspective on how malware detection techniques have evolved and where current research efforts are most actively directed. The synthesized insights provide researchers and practitioners with a clearer understanding of the existing landscape and a solid foundation for further study and practical implementation. Despite its breadth, the review recognizes several limitations. Malware continues to evolve rapidly, and new variants or detection strategies may have emerged beyond the timeline of this study. Additionally, meaningful comparison across existing research remains difficult due to inconsistencies in datasets, evaluation metrics, and experimental setups. Although AI and deep learning–based models receive considerable attention, challenges related to reproducibility, dataset imbalance, and the absence of standardized benchmarks still hinder the generalization of reported results. Looking ahead, future work should prioritize the development of unified evaluation frameworks and benchmark datasets to facilitate more consistent and comparable assessments of detection methods. Further research is also warranted in areas such as model explainability, real-time detection performance, adversarial robustness, and cross-platform adaptability. Advancing hybrid detection architectures, reducing the computational demands of

deep learning models, and integrating automated model optimization techniques such as AutoML and evolutionary algorithms, represent promising directions. Strengthening these research avenues will support the creation of more resilient, scalable, and adaptive malware defense mechanisms capable of keeping pace with evolving cyber threats.

Acknowledgement: Not applicable.

Funding Statement: This research was funded by the European University of Atlantic.

Authors Contributions: M. Mohsin Raza: conceptualization, data curation, writing—the original draft; Muhammad Umair: formal analysis, conceptualization, writing—the original draft; Imran Arshad Choudhry: methodology, formal analysis, data curation; Muhammad Qasim: software, methodology, project administration; Muhammad Tahir Naseem: visualization, software, formal analysis; Mamoona Naveed Asghar: data curation, methodology, validation; Daniel Gavilanes: funding acquisition, investigation, visualization; Manuel Masias Vergara: investigation, resources; visualization; Imran Ashraf: supervision, validation, writing—review and editing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethic Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Supplementary Materials: The supplementary material is available online at https://www.techscience.com/doi/10.32604/cmes.2025.074164/s1.

References

1. Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. J Big Data. 2020;7(1):41. doi:10.1186/s40537-020-00318-5.
2. Bagui L, Lusinga S, Pule N, Tuyeni T, Mtegha CQ, Calandro E, et al. The impact of COVID-19 on cybersecurity awareness-raising and mindset in the southern African development community (SADC). Electron J Inf Syst Dev Ctries. 2023;89(4):e12264. doi:10.1002/isd2.12264.
3. Kalinaki K. Ransomware threat mitigation strategies for protecting critical infrastructure assets. In: Ransomware evolution. Boca Raton, FL, USA: CRC Press; 2024. p. 120–43.
4. Aleroud A, Zhou L. Phishing environments, techniques, and countermeasures: a survey. Comput Secur. 2017;68:160–96.
5. Krishnapriya S, Singh S. A comprehensive survey on advanced persistent threat (APT) detection techniques. Comput Mater Contin. 2024;80(2):2675.
6. Thawait N. Machine learning in cybersecurity: applications, challenges and future directions. Int J Sci Res Comput Sci Eng Inf Technol. 2024;10:16–27. doi:10.32628/cseit24102125.
7. Truong TC, Zelinka I, Plucar J, Candik M, Šulc V. Artificial intelligence and cybersecurity: past, presence, and future. In: Artificial intelligence and evolutionary computations in engineering systems. Singapore: Springer; 2020. p. 351–63. doi:10.1007/978-981-15-0199-9_30.
8. Lund BD, Lee TH, Wang Z, Wang T, Mannuru NR. Zero trust cybersecurity: procedures and considerations in context. Encyclopedia. 2024;4(4):1520–33. doi:10.3390/encyclopedia4040099.
9. Anderson HS, Roth P. Ember: an open dataset for training static PE malware machine learning models. arXiv: 1804.04637. 2018.
10. Martín I, Hernández JA, de los Santos S. Machine-learning based analysis and classification of Android malware signatures. Future Gener Comput Syst. 2019;97:295–305. doi:10.1016/j.future.2019.03.006.
11. Odii J, Hampo J, Onwuama N. Comparative analysis of malware detection techniques using signature, behaviour and heuristics. Int J Comput Sci Inf Secur. 2019;17:33–50.

12. Li N, Zhang Z, Che X, Guo Z, Cai J. A survey on feature extraction methods of heuristic malware detection. J Phys Conf Ser. 2021;1757(1):012071. doi:10.1088/1742-6596/1757/1/012071.
13. Francisco Montes JBH. Detecting malware in cyberphysical systems using machine learning: a survey. KSII Trans Internet Inf Syst. 2021;15(3):1–15.
14. Dey AK, Gupta GP, Sahu SP. Hybrid meta-heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks. Procedia Comput Sci. 2023;218:318–27. doi:10.1016/j.procs.2023.01.014.
15. Gopinath M, Sethuraman SC. A comprehensive survey on deep learning based malware detection techniques. Comput Sci Rev. 2023;47:100529. doi:10.1016/j.cosrev.2022.100529.
16. Yunmar RA, Kusumawardani SS, Widyawan, Mohsen F. Hybrid android malware detection: a review of heuristic-based approach. IEEE Access. 2024;12:41255–86. doi:10.1109/access.2024.3377658.
17. Raj M, Angel Arul Jothi J. Hybrid approach for phishing website detection using classification algorithms. ParadigmPlus. 2022;3:16–29. doi:10.55969/paradigmplus.v3n3a2.
18. Ozkan-Okay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, et al. A comprehensive survey: evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEE Access. 2024;12:12229–56. doi:10.1109/access.2024.3355547.
19. Ofusori L, Bokaba T, Mhlongo S. Artificial intelligence in cybersecurity: a comprehensive review and future direction. Appl Artif Intell. 2024;38(1):2439609. doi:10.1080/08839514.2024.2439609.
20. Habib F, Shirazi SH, Aurangzeb K, Khan A, Bhushan B, Alhussein M. Deep neural networks for enhanced security: detecting metamorphic malware in IoT devices. IEEE Access. 2024;12:48570–82. doi:10.1109/access.2024.3383831.
21. Gaber MG, Ahmed M, Janicke H. Malware detection with artificial intelligence: a systematic literature review. ACM Comput Surv. 2024;56(6):1–33. doi:10.1145/3638552.
22. Dhanushkodi K, Thejas S. AI enabled threat detection: leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access. 2024;12:173127–36. doi:10.1109/access.2024.3493957.
23. Bensaoud A, Kalita J, Bensaoud M. A survey of malware detection using deep learning. Mach Learn Appl. 2024;16:100546. doi:10.1016/j.mlwa.2024.100546.
24. Alketbi KS, Mehmood A. A comprehensive survey of explainable artificial intelligence techniques for malicious insider threat detection. IEEE Access. 2025;13:121772–98. doi:10.1109/access.2025.3587114.
25. Chandran S, Syam SR, Sankaran S, Pandey T, Achuthan K. From static to AI-driven detection: a comprehensive review of obfuscated malware techniques. IEEE Access. 2025;13:74335–58. doi:10.1109/access.2025.3550781.
26. Binbeshr F, Imam M, Ghaleb M, Hamdan M, Rahim MA, Hammoudeh M. The rise of cognitive SOCs: a systematic literature review on AI approaches. IEEE Open J Comput Soc. 2025;6:360–79. doi:10.1109/ojcs.2025.3536800.
27. Ankalaki S, Atmakuri AR, Pallavi M, Hukkeri GS, Jan T, Naik GR. Cyber attack prediction: from traditional machine learning to generative artificial intelligence. IEEE Access. 2025;13:44662–706. doi:10.1109/access.2025.3547433.
28. Alshoulie M, Mehmood A. Deep learning approaches for malware detection: a comprehensive review of techniques, challenges, and future directions. IEEE Access. 2025;13:118652–77. doi:10.1109/access.2025.3582875.
29. Wu Y, Zhuang H, Jia Y, Zhang Y. A survey of machine learning approaches for malware detection. In: CNSSE '25: Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering; 2025 Feb 21–23; Qingdao, China. p. 269–73.
30. Ferdous J, Islam R, Mahboubi A, Islam MZ. A survey on ML techniques for multi-platform malware detection: securing PC, mobile devices, IoT, and cloud environments. Sensors. 2025;25(4):1153. doi:10.3390/s25041153.
31. Song Y, Zhang D, Wang J, Wang Y, Wang Y, Ding P. Application of deep learning in malware detection: a review. J Big Data. 2025;12(1):99.
32. Goyal M, Kumar R. The pipeline process of signature-based and behavior-based malware detection. In: Proceedings of the 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA); 2020 Oct 30–31; Greater Noida, India. p. 497–502.
33. Joe WJ, Kim HS. A greedy algorithm for generating malware signatures based on association. In: Proceedings of the 2022 IEEE International Conference on Big Data and Smart Computing (BigComp); 2022 Jan 17–20; Daegu, Republic of Korea. p. 52–5.

34. Pang Y, Chen Z, Peng L, Ma K, Zhao C, Ji K. A signature-based assistant random oversampling method for malware detection. In: Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE); 2019 Aug 5–8; Rotorua, New Zealand. p. 256–63.
35. Al-Asli M, Ghaleb TA. Review of signature-based techniques in antivirus products. In: Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS); 2019 Apr 3–4; Sakaka, Saudi Arabia. p. 1–6.
36. Nahmias D, Cohen A, Nissim N, Elovici Y. TrustSign: trusted malware signature generation in private clouds using deep feature transfer learning. In: Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN); 2019 Jul 14–19; Budapest, Hungary. p. 1–8.
37. Tirumala SS, Valluri MR, Nanadigam D. Evaluation of feature and signature based training approaches for malware classification using autoencoders. In: Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS); 2020 Jan 7–11; Bengaluru, India. p. 1–5.
38. Shi Z, Wang X, Liu P. NBP-MS: malware signature generation based on network behavior profiling. In: Proceedings of the 2022 26th International Conference on Pattern Recognition (ICPR); 2022 Aug 21–25; Montreal, QC, Canada. p. 1865–70.
39. Odat E, Yaseen QM. A novel machine learning approach for android malware detection based on the co-existence of features. IEEE Access. 2023;11:15471–84. doi:10.1109/access.2023.3244656.
40. Afreen A, Aslam M, Ahmed S. Analysis of fileless malware and its evasive behavior. In: Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS); 2020 Oct 20–21; Islamabad, Pakistan. p. 1–8.
41. Alkhateeb EM, Stamp M. A dynamic heuristic method for detecting packed malware using Naive Bayes. In: Proceedings of the 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA); 2019 Nov 19–21; Ras Al Khaimah, United Arab Emirates. p. 1–6.
42. Almeida R, Westphall C. Heuristic phishing detection and URL checking methodology based on scraping and web crawling. In: Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI); 2020 Nov 9–10; Arlington, VA, USA. p. 1–6.
43. Chavan A, Kerakalamatti K, Srivastva S. Implementation of portable antivirus system using signature-based detection and heuristic analysis. In: Proceedings of the 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI); 2021 Jun 3–5; Tirunelveli, India. p. 1481–6.
44. Dou J, Zhang Y, Shi Y, Jiang L. Improved N-gram algorithm for unknown malware detection. In: Proceedings of the 2022 International Conference on Machine Learning, Cloud Computing and Intelligent Mining (MLCCIM); 2022 Aug 5–7; Xiamen, China. p. 165–70.
45. Arora L, Thakur N, Yadav SK. USB rubber ducky detection by using heuristic rules. In: Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS); 2021 Feb 19–20; Greater Noida, India. p. 156–60.
46. Zhang H, Luo S, Zhang Y, Pan L. An efficient android malware detection system based on method-level behavioral semantic analysis. IEEE Access. 2019;7:69246–56. doi:10.1109/access.2019.2919796.
47. Tanana D, Tanana G. Advanced behavior-based technique for cryptojacking malware detection. In: Proceedings of the 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS); 2020 Dec 14–16; Adelaide, SA, Australia. p. 1–4.
48. Abderrahmane A, Adnane G, Yacine C, Khireddine G. Android malware detection based on system calls analysis and CNN classification. In: Proceedings of the 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW); 2019 Apr 15–18; Marrakech, Morocco. p. 1–6.
49. Aslan O, Ozkan-Okay M, Gupta D. Intelligent behavior based malware detection system on cloud computing environment. IEEE Access. 2021;9:83252–71. doi:10.1109/access.2021.3087316.
50. Du D, Sun Y, Ma Y, Xiao F. A novel approach to detect malware variants based on classified behaviors. IEEE Access. 2019;7:81770–82. doi:10.1109/access.2019.2924331.
51. Jang M, Lee K. An advanced approach for detecting behavior-based intranet attacks by machine learning. IEEE Access. 2024;12:52480–95. doi:10.1109/access.2024.3387016.

52. Feng R, Chen S, Xie X, Meng G, Lin SW, Liu Y. A performance-sensitive malware detection system using deep learning on mobile devices. IEEE Trans Inf Forensic Secur. 2021;16(7):1563–78. doi:10.1109/tifs.2020.3025436.
53. Ibrahim WNH, Anuar S, Selamat A, Krejcar O, Gonzalez Crespo R, HerreraViedma E, et al. Multilayer framework for botnet detection using machine learning algorithms. IEEE Access. 2021;9:48753–68. doi:10.1109/access.2021.3060778.
54. Ali M, Shahroz M, Mushtaq MF, Alfarhood S, Safran M, Ashraf I. Hybrid machine learning model for efficient botnet attack detection in IoT environment. IEEE Internet Things J. 2024;2(12):1–22. doi:10.1109/access.2024.3376400.
55. Hussain F, Abbas SG, Pires IM, Tanveer S, Fayyaz UU, Garcia NM, et al. A two-fold machine learning approach to prevent and detect IoT botnet attacks. IEEE Access. 2021;9:163412–30. doi:10.1109/access.2021.3131014.
56. Roseline SA, Geetha S, Kadry S, Nam Y. Intelligent vision-based malware detection and classification using deep random forest paradigm. IEEE Access. 2020;8:206303–24. doi:10.1109/access.2020.3036491.
57. Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Venkatraman S. Robust intelligent malware detection using deep learning. IEEE Access. 2019;7:46717–38. doi:10.1109/access.2019.2906934.
58. Ajvad Haneef K, Madhu Kumar SD. Deep learning techniques for malware detection: a comprehensive survey. In: Proceedings of the 2023 International Conference on Computer, Electronics & Electrical Engineering & Their Applications (IC2E3); 2023 Jun 8–9; Srinagar Garhwal, India. p. 1–7.
59. Liu Y, Fan H, Zhao J, Zhang J, Yin X. Efficient and generalized image-based CNN algorithm for multi-class malware detection. IEEE Access. 2024;12:104317–32. doi:10.1109/access.2024.3435362.
60. Kwan LM. Markov image with transfer learning for malware detection and classification. In: Proceedings of the IEEE Region 10 Annual International Conference, Proceedings/TENCON; 2022 Nov 1–4; Hong Kong, China.
61. Baptista I, Shiaeles S, Kolokotronis N. A novel malware detection system based on machine learning and binary visualization. In: Proceedings of the 2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019; 2019 May 20–24; Shanghai, China. p. 1–6.
62. Dharmalaksana PS, Mantoro T, Khakim L, Nurseno M. Improved malware detection results using visualization-based detection techniques and convolutional neural network. In: Proceedings of the 2022 IEEE 8th International Conference on Computing, Engineering and Design, ICCED 2022; 2022 Jul 28–29; Sukabumi, Indonesia. p. 1–5.
63. Gebrehans G, Ilyas N, Eledlebi K, Lunardi WT, Andreoni M, Yeun CY, et al. Generative adversarial networks for dynamic malware behavior: a comprehensive review, categorization, and analysis. IEEE Trans Artif Intell. 2025;6(8):1955–76. doi:10.1109/tai.2025.3537966.
64. Botacin M, Alves MZ, Oliveira D, Grégio A. HEAVEN: a hardware-enhanced AntiVirus ENgine to accelerate real-time, signature-based malware detection. Expert Syst Appl. 2022;201:117083. doi:10.1016/j.eswa.2022.117083.
65. Usman N, Usman S, Khan F, Jan MA, Sajid A, Alazab M, et al. Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. Future Gener Comput Syst. 2021;118:124–41. doi:10.1016/j.future.2021.01.004.
66. Pinhero A, Anupama ML, Vinod P, Visaggio CA, Aneesh N, Abhijith S, et al. Malware detection employed by visualization and deep neural network. Comput Secur. 2021;105:102247.
67. Tekerek A, Yapici MM. A novel malware classification and augmentation model based on convolutional neural network. Comput Secur. 2022;112:102515. doi:10.1016/j.cose.2021.102515.
68. Fan M, Li S, Han W, Wu X, Gu Z, Tian Z. A novel malware detection framework based on weighted heterograph. In: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies (CIAT 2020); 2021 Dec 4–6; Guangzhou, China. p. 39–43.
69. Omar M. New approach to malware detection using optimized convolutional neural network. In: Machine learning for cybersecurity. Cham, Switzerland: Springer International Publishing; 2022. p. 13–35. doi:10.1007/978-3-031-15893-3_2.
70. Ahmed SR, Mohamed SJ, Aljanabi MS, Algburi S, Majeed DA, Kurdi NA, et al. A novel approach to malware detection using machine learning and image processing. In: Proceedings of the Cognitive Models and Artificial Intelligence Conference, AICCONF '24; 2024 May 25–26; Istanbul, Turkiye. New York, NY, USA: Association for Computing Machinery; 2024. p. 298–302.

71. Nataraj L, Karthikeyan S, Jacob G, Manjunath BS. Malware images: visualization and automatic classification. In: Proceedings of the 8th International Symposium on Visualization for Cyber Security, VizSec '11; 2011 Jul 20; Pittsburgh, PA, USA. New York, NY, USA: Association for Computing Machinery; 2011. p. 1–7.
72. He P, Xia Y, Zhang X, Ji S. Efficient query-based attack against ML-based android malware detection under zero knowledge setting. In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS '23; 2023 Nov 26–30; Copenhagen, Denmark. New York, NY, USA: Association for Computing Machinery; 2023. p. 90–104.
73. Selvaraj PA, Jagadeesan M, Saravanan TM, Kumar A, Kumar A, Singh MK. Comparative study of detection and analysis of different malware with the help of different algorithm. In: 2023 International Conference on Computer Communication and Informatics (ICCCI); 2023 Jan 23–25; Coimbatore, India. p. 1–6.
74. Sihag V, Swami A, Vardhan M, Singh P. Signature based malicious behavior detection in android. In: International Conference on Computing Science, Communication and Security; 2020 Mar 26–27; Gujarat, India. Singapore: Springer; 2020. p. 251–62.
75. Anisetti M, Ardagna C, Bena N, Giandomenico V, Gianini G. Lightweight behavior-based malware detection. In: Management of Digital EcoSystems; 2023 May 5–7; Heraklion, Greece. Cham, Switzerland: Springer Nature; 2024. p. 237–50. doi:10.1007/978-3-031-51643-6_17.
76. Joshi C, Kumar J, Kumawat G. Detection of unseen malware threats using generative adversarial networks and deep learning models. Sci Rep. 2025;15(1):34804. doi:10.1038/s41598-025-18811-3.
77. Kwon HY, Kim T, Lee MK. Advanced intrusion detection combining signature-based and behavior-based detection methods. Electronics. 2022;11(6):867. doi:10.3390/electronics11060867.
78. Alomari ES, Nuiaa RR, Alyasseri ZAA, Mohammed HJ, Sani NS, Esa MI, et al. Malware detection using deep learning and correlation-based feature selection. Symmetry. 2023;15(1):123. doi:10.3390/sym15010123.
79. An BY, Yang J, Kim S, Kim T. Malware detection using dual siamese network model. Comput Model Eng Sci. 2024;141(1):563–84.
80. Kil Y, Jeon Y, Lee S, Lee I. Multi-binary classifiers using optimal feature selection for memory-saving intrusion detection systems. Comput Model Eng Sci. 2024;141(2):1473–93. doi:10.32604/cmes.2024.052637.
81. Al-Ghanem WK, Qazi EUH, Zia T, Faheem MH, Imran M, Ahmad I. Malware detection using attention based deep neural networks. Comput Model Eng Sci. 2025;143(1):60444.
82. Assegie TA. An optimized KNN model for signature-based malware detection. Int J Comput Eng Res Trends. 2021;8(2):46–9.
83. Ojugo A, Eboka A. Signature-based malware detection using approximate boyer moore string matching algorithm. Int J Math Sci Comput. 2019;5:49–62. doi:10.5815/ijmsc.2019.03.05.
84. Udayakumar N, Anandaselvi S, Subbulakshmi T. Dynamic malware analysis using machine learning algorithm. In: Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS); 2017 Dec 7–8; Palladam, India. p. 795–800.
85. Chakravarty AK, Raj A, Paul S, Apoorva S. A study of signature-based and behaviour-based malware detection approaches. Int J Adv Res Ideas Innov Technol. 2019;5(3):1509–11.
86. Fouad MA, Abdel-Hamid AT. On detecting IoT power signature anomalies using hidden markov model (HMM). In: Proceedings of the 2019 31st International Conference on Microelectronics (ICM); 2019 Dec 15–18; Cairo, Egypt. p. 108–12.
87. Cisar P, Joksimovic D. Heuristic scanning and sandbox approach in malware detection. Archibald Reiss Days. 2019;9(2):425–35.
88. Sharma RM, Agrawal CP. MH-DLdroid: a meta-heuristic and deep learning-based hybrid approach for android malware detection. Int J Intell Eng Syst. 2022;15(4):299–308.
89. Jhansi KS, Chakravarty S, Varma PRK. A two-tier fuzzy meta-heuristic hybrid optimization for dynamic android malware detection. SN Comput Sci. 2022;4(2):117.
90. Suryati OT, Budiono A. Impact analysis of malware based on call network API with heuristic detection method. Int J Adv Data Inf Syst. 2020;1(1):1–8. doi:10.25008/ijadis.v1i1.176.

91. Hajmasan G, Mondoc A, Cret O. Bytecode heuristic signatures for detecting malware behavior. In: Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp); 2019 Sep 19–21; Moka, Mauritius. p. 1–6.
92. Raja AS, Pradeepa G, Arulkumar N. Mudhr: malicious URL detection using heuristic rules based approach. AIP Conf Proc. 2022;2393(1):020176. doi:10.1063/5.0074077.
93. Samarthrao KV. A hybrid meta-heuristic-based multi-objective feature selection with adaptive capsule network for automated email spam detection. Int J Intell Robot Appl. 2021;6:497–521. doi:10.1007/s41315-021-00217-9.
94. Bhuiyan FA, Brown KE, Sharif MB, Johnson QD, Talbert DA. Assessing modality selection heuristics to improve multimodal machine learning for malware detection. In: The Thirty-Third International Flairs Conference; 2023 May 14–17; Clearwater Beach, FL, USA. p. 434–7.
95. Lu T, Du Y, Ouyang L, Chen Q, Wang X. Android malware detection based on a hybrid deep learning model. Secur Commun Netw. 2020;2020:1–11. doi:10.1155/2020/8863617.
96. Xu Q, Zhao D, Yang S, Xu L, Li X. Android malware detection based on behavioral-level features with graph convolutional networks. Electronics. 2023;12(23):4817. doi:10.1109/aips64124.2024.00027.
97. Muhtadi AF, Almaarif A. Analysis of malware impact on network traffic using behavior-based detection technique. Int J Adv Data Inform Syst. 2020;1(1):17–25. doi:10.25008/ijadis.v1i1.8.
98. Shakya S, Dave M. Analysis, detection, and classification of android malware using system calls. arXiv:2208.06130. 2022.
99. Singh J, Singh J. Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms. Inf Softw Tech. 2020;121:106273. doi:10.1016/j.infsof.2020.106273.
100. Sun Y, Bashir AK, Tariq U, Xiao F. Effective malware detection scheme based on classified behavior graph in IIoT. Ad Hoc Netw. 2021;120:102558. doi:10.1016/j.adhoc.2021.102558.
101. Rosli NA, Yassin W, Ma F, Selamat SR. Clustering analysis for malware behavior detection using registry data. Int J Adv Comput Sci Appl. 2019;10(12):93–102. doi:10.14569/ijacsa.2019.0101213.
102. Kumar N, Mukhopadhyay S, Gupta M, Handa A, Shukla SK. Malware classification using early stage behavioral analysis. In: Proceedings of the 2019 14th Asia Joint Conference on Information Security (AsiaJCIS); 2019 Aug 1–2; Kobe, Japan. p. 16–23.
103. Khammas BM. Ransomware detection using random forest technique. ICT Express. 2020;6(4):325–31. doi:10.1016/j.icte.2020.11.001.
104. Fallah S, Bidgoly AJ. Android malware detection using network traffic based on sequential deep learning models. Softw Pract Exp. 2022;52(9):1987–2004. doi:10.1002/spe.3112.
105. Kumari K, Mrunalini M. Detecting denial of service attacks using machine learning algorithms. J Big Data. 2022;9(1):56. doi:10.1186/s40537-022-00616-0.
106. Hwang J, Kim J, Lee S, Kim K. Two-stage ransomware detection using dynamic analysis and machine learning techniques. Wirel Pers Commun. 2020;112(4):2597–609. doi:10.1007/s11277-020-07166-9.
107. Bae SI, Lee GB, Im EG. Ransomware detection using machine learning algorithms. Concurr Comput. 2020;32(18):e5422. doi:10.1002/cpe.5422.
108. Saridou B, Moulas I, Shiaeles S, Papadopoulos B. Image-based malware detection using α-cuts and binary visualisation. Appl Sci. 2023 Apr;13(7):4624. doi:10.3390/app13074624.
109. Ghahramani M, Taheri R, Shojafar M, Javidan R, Wan S. Deep image: a precious image based deep learning method for online malware detection in IoT environment. Internet Things. 2024;27:101300. doi:10.1016/j.iot.2024.101300.
110. Naeem H, Ullah F, Naeem MR, Khalid S, Vasan D, Jabbar S, et al. Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. Ad Hoc Netw. 2020;105:102154. doi:10.1016/j.adhoc.2020.102154.
111. Sihwail R, Omar K, Akram K. An effective memory analysis for malware detection and classification. Comput Mater Contin. 2021;67(2):2301–20.
112. Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Rep. 2021;7:8176–86. doi:10.1016/j.egyr.2021.08.126.

113. Zhang Y, Gao C, Wu Y, Dou S, Wu C, Zhang Y, et al. Fighting fire with fire: continuous attack for adversarial android malware detection. In: Proceedings of the 34th USENIX Conference on Security Symposium, SEC '25; 2025 Aug 13–15; Seattle, WA, USA. p. 4897–916.
114. Tricco AC, Lillie E, Zarin W, O'Brien KK, Colquhoun H, Levac D, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Ann Intern Med. 2018;169(7):467–73. doi:10.7326/m18-0850.
115. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. EBSE Tech Rep. 2007;22(1):58–65.
116. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering; 2014 May 13–14; London, UK. p. 1–10.
117. Ferdous J, Islam R, Mahboubi A, Zahidul Islam M. AI-based ransomware detection: a comprehensive review. IEEE Access. 2024;12:136666–95. doi:10.1109/access.2024.3461965.
118. Altulaihan E, Alismail A, Hafizur Rahman MM, Ibrahim AA. Email security issues, tools, and techniques used in investigation. Sustainability. 2023;15(13):10612. doi:10.3390/su151310612.
119. Razaulla S, Fachkha C, Markarian C, Gawanmeh A, Mansoor W, Fung BCM, et al. The age of ransomware: a survey on the evolution, taxonomy, and research directions. IEEE Access. 2023;11:40698–723. doi:10.1109/access.2023.3268535.
120. Stafiniak M, Wodo W. State-sponsored cybersecurity attacks. In: 2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS); 2022 Oct 6–7; Riga, Latvia. p. 1–6. doi:10.1109/ITMS56974.2022.9937131.
121. Muniandy M, Ismail N, Al-Nahari A, Yao DN. Evolution and impact of ransomware: patterns, prevention, and recommendations for organizational resilience. Int J Acad Res Bus Soc Sci. 2024;14(1):585–99.
122. Kamdan, Pratama Y, Munzi RS, Mustafa AB, Kharisma IL. Static malware detection and classification using machine learning: a random forest approach. Eng Proc. 2025;107(1):76. doi:10.3390/engproc2025107076.
123. Sharma U, Anjum A. Malware analysis using static and dynamic analysis. In: Swaroop A, Virdee B, Correia SD, Polkowski Z, editors. Proceedings of Data Analytics and Management; 2025 Jun 13–15; London, UK. Cham, Switzerland: Springer Nature; 2025. p. 517–25. doi:10.1007/978-3-032-03072-6_41.
124. Hossain F, Islam MN, Islam MA, Ali MM, Muntasir F, Mahiuddin M. A synergistic approach to detect malicious behaviour through correlation-based feature selection with deep learning. In: Proceedings of the 2025 International Conference on Electrical, Computer and Communication Engineering (ECCE); 2025 Feb 13–15; Chittagong, Bangladesh. p. 1–6.
125. Thompson M, Patel R, Jimenez C, Chen ML, Okoro D, Andrew J. Comparative study of signature-based vs AI-based malware detection; 2022. [cited 2025 Jan 1]. Available from: https://www.researchgate.net/publication/391857720_Comparative_Study_of_Signature-Based_vs_AI-Based_Malware_Detection.
126. Elkilany AR, Chu YB. Elucidation on the performance of various machine learning models for real-time malware detection, malware classification and network packet screening. Mach Learn Comput Sci Eng. 2025;1(1):9. doi:10.1007/s44379-024-00010-y.
127. Chang KY, Seo CJ. Static analysis and machine learning-based malware detection using PE-header features and stacking ensemble. Int J Intell Revol Sci Syst. 2025;8(2):690–702.
128. Akhtar MS, Feng T. Evaluation of machine learning algorithms for malware detection. Sensors. 2023;23(2):946. doi:10.3390/s23020946.
129. Pathak A, Barman U, Kumar S. Machine learning approach to detect Android malware using feature-selection based on feature importance score. J Eng Res. 2025;13(2):712–20. doi:10.1016/j.jer.2024.04.008.
130. Ali S, Abdulrazzaq M, Gaata M. Learning techniques-based malware detection: a comprehensive review. Mesopotamian J CyberSecur. 2025;5:273–300. doi:10.58496/mjcs/2025/018.
131. Gorment AS, Krejcar O. Machine learning algorithm for malware detection taxonomy current challenges and future directions. IEEE Access. 2023;11:141045–89. doi:10.1109/access.2023.3256979.
132. Kumar A, Sachan RK. Automated machine learning for malware detection. In: ICT for intelligent systems. Singapore: Springer Nature; 2025. p. 1–12. doi:10.1007/978-981-96-8796-1_1.

133. Han K, Lim JH, Im EG. Malware analysis method using visualization of binary files. In: Proceedings of the 2013 Research in Adaptive and Convergent Systems, RACS 2013; 2013 Oct 1–3; Montreal, QC, Canada. p. 317–21.
134. Venkatraman S, Alazab M, Vinayakumar R. A hybrid deep learning image-based analysis for effective malware detection. J Inf Secur Appl. 2019;47:377–89. doi:10.1016/j.jisa.2019.06.006.
135. Ni S, Qian Q, Zhang R. Malware identification using visualization images and deep learning. Comput Secur. 2018;77:871–85.
136. Singh P, Priyanshu, Bhat A. Malware classification using malware visualization and deep learning. In: Proceedings of the 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC); 2023 May 4–6; Salem, India. p. 528–34.
137. Conti M, Losiouk E, Visintin A. What you see is not what you get: a man-in-the-middle attack applied to video channels. In: SAC '22: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing; 2022 Apr 25–29; Virtual. p. 1723–6.
138. Famera A, Hilger B, Bhunia S, Heil P. Analyzing the mirai IoT botnet and its recent variants: Satori, Mukashi, Moobot, and Sonic. arXiv:2508.01909. 2025.
139. Ma R, Yin S, Feng X, Zhu H, Sheng VS. A lightweight deep learning-based android malware detection framework. Expert Syst Appl. 2024;255:124633. doi:10.1016/j.eswa.2024.124633.
140. Li H, Yao Z, Wu B, Gao C, Xu T, Yuan W, et al. Automated mass malware factory: the convergence of piggybacking and adversarial example in Android malicious software generation. In: Proceedings of the 32nd Network and Distributed System Security Symposium; 2025 Feb 24–28; San Diego, CA, USA.