European Journal of Computer Science and Information Technology, 13(52),13-33, 2025

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

AI-Driven Malware Detection and Classification: A Systematic Review of Techniques and Effectiveness

Ismail Adeyemi

doi: https://doi.org/10.37745/ejcsit.2013/vol13n521333 Published October 06, 2025

Citation: Adeyemi I. (2025) AI-Driven Malware Detection and Classification: A Systematic Review of Techniques and Effectiveness, *European Journal of Computer Science and Information Technology*, 13(52),13-33

Abstract: *In addition to classifying malware, it was further observed that malware analysis experts have developed new methodologies and strategies to assess the composition of malware samples by comparing their behavior and features to several known malware families. Thus, this study examined AI-driven malware detection and classification, using the systematic review of literature to understand the techniques and effectiveness of the AI systems. The study adopted the meta-synthesis research design. Meanwhile, the PRISMA chart was used for the selection of literature. There were identified inclusion and exclusion criteria that were outlined to determine the literature that are relevant to the study. Results showed that the techniques used in AI-driven malware detection and classification systems include deep learning techniques, machine learning techniques, and hybrid models. The findings showed that the AI-driven malware detection and classification system is highly effective in detecting and classifying malware. Findings of the study showed that the evaluation strategies for AI-driven malware detection and classification include standard metrics, benchmark datasets, experimental comparisons, and cross-validation. Results showed that the challenges associated with the use AI-enhanced systems to detect and classify malware include computational complexity, interpretability, dataset limitations, adversarial attacks, and real-time deployment constraints. The study concludes that AI-driven malware detection and classification systems have different techniques and they are highly effective. It was recommended that there is a need for continuous update of datasets to reflect new attack vectors.*

Keywords: Malware, AI-driven malware, malware detection, malware classification, artificial intelligence (AI)

INTRODUCTION

Generally, malware is one of the most pervasive and damaging forms of attack in the rapidly evolving landscape of cybersecurity threats. It is capable of compromising systems, which can lead to stealing of sensitive data and disrupting important infrastructures. In recent times, there has been a common shift from traditional signature-based and heuristic methods of malware detection

to a more sophisticated and diverse modern malware variant. Thus, it has become increasingly challenging and that has led to the widespread use of artificial intelligence (AI)-driven malware detection and classification. This AI-driven approaches are common with the use of machine learning (ML) and deep learning (DL), which offer the potential of threat identification, attack vector adaptation, and high-speed accurate processing of large volumes of data that may not be possible with traditional signature-based and heuristic methods of malware detection.

Aslan and Samet (2020) referred to malware detection as the act of figuring out whether or not a particular application has malicious intent. The authors noted that malware was first detected using a signature-based detection technique, which has shortcomings including inability to identify malware that is unknown or of a fresh generation. They highlighted that there are different approaches that have been proposed including behavioral-, heuristic-, and model checking-based detection. Aside these approaches, others have also been proposed including deep learning-, cloud-, mobile devices-, and IoT-based detection. Aboaoja et al. (2022) noted that behavioral-based approach can be evaded by malware that can discriminate between analytic environment and the actual machine environment. It was noted further that malware detection and classification models using automated or manual criteria increase the accuracy of malware detection.

McLaughlin et al. (2017) mentioned that malware detection techniques can be divided into three categories, which include signature based, heuristic based, and specification based. These techniques can either be traditional or AI-driven. In contrast to traditional techniques, machine learning-based detection can identify malware that have not yet been discovered and can offer superior efficacy and efficiency (Liu et al., 2020). Ye et al. (2017) averred that the development of intelligent techniques for successful and efficient malware detection from the actual and extensive daily sample collection is required to manage or reduce the rise in malware samples. As malware detection techniques advance, malware detectors employ a variety of strategies to prevent the catastrophic impacts of these programs. Malware detectors are used to identify these malwares, and antivirus scanners are one method to identify some of them (Tahir, 2018).

Android OS has dominated the worldwide smart phone, which has some malicious software that can exploit data and privacy on Android devices (Hsieh et al., 2015). Damodaran et al. (2017) noted that that Android malware detection technology can be categorized into static detection, dynamic detection, and hybrid detection. These categories are the analysis approaches that may be employed in malware detection. According to Anderson et al. (2017), static malware detection has been in use since at least 2001 and is a crucial component of a security system as, when done correctly, it may identify malicious files before they are executed. For example, when an existing file undergoes modification when it is written to disk, or when it is asked to execute. Liu et al. (2020) noted that dynamic detection entails the analysis of applications by running the code. Although dynamic detection requires a comparatively large amount of time and processing resources, it can reveal risks that are difficult to identify with static analysis. In order to identify

behavior or malicious functionality in programs, hybrid approaches include run-time data from dynamic analysis into a static analysis technique (Rao & Hande, 2017).

Abusitta et al. (2021) observed that deep learning models are applied to improve malware classification accuracy in both detection and classification. In addition to classifying malware, it was further observed that malware analysis experts have developed new methodologies and strategies to assess the composition of malware samples by comparing their behavior and features to several known malware families. Aslan and Yilmaz (2021) described malware classification as a step further to malware detection. The authors noted that malware classification is the determination of the category or family of malware after a file has been identified as malware. Cakir and Dogdu (2018) noted that there are two stages of malware analysis. The first phase is the malware detection phase, which concerns the initial detection and identification of malware. Malware classification phase concerns the security systems attempt to identify or categorize every threat sample as belonging to one of the relevant malware families during the second phase. In malware classification, the feature vector selection techniques are employed, which may be categorized into static and dynamic analysis (Islam et al., 2013).

Having established that the malware technology analysis for malware classification comprises of static and dynamic analysis, there are no hybrid analysis approach compared to malware detection. This provides that malware classification integrates run-time data from dynamic analysis into a static analysis technique (Chanajitt et al., 2021). Meanwhile, malware classification can be carried out using a wide variety of machine learning classifiers, which include logistic regression, neural networks, and decision trees (Pascanu et al., 2015). When compared to traditional learning algorithms, Convolutional Neural Networks (CNN), a deep learning technique, have demonstrated better performance, particularly in applications like image classification. Moreover, it was established that Microsoft malware and Malimg malware outperform the state-of-the-art performance on the difficult malware classification datasets (Kalash et al., 2018).

The continuous growth in technological development has led to a concerning increase in the incidence and sophistication of malware attacks. For instance, the traditional malware detection techniques, such as polymorphic and zero-day malware, are not capable of detecting the newly developed malware (Deldar & Abadi, 2023). Therefore, there is a need for a more intelligent solutions, which is an AI-enhanced malware detection and classification approaches. These AI-enhanced approaches are engineered through machine learning and deep learning systems, which offer a dynamic approach for enhancing malware detection and classification (Faiz et al., 2025). Studies (e.g., Chandran et al., 2025; Moamin et al., 2025) have proposed different AI-based methods, a comprehensive understanding of the techniques and effectiveness remains unknown. Moreover, the datasets associated with some of the AI-driven models proposed and tested are limited or outdated, which raises concerns about generalizability and real-world performance. This performance may influence the effectiveness in the long-run. It is against the foregoing that this

study seeks to examine AI-driven malware detection and classification with a focus on the techniques and effectiveness of those AI-models that have been proposed. The research questions for this systematic review are:

1. What is the AI-driven techniques used in malware detection and classification?
2. What is the effectiveness of the AI-driven malware detection and classification approaches?
3. What are the evaluation strategies for AI-based malware detection and classification systems?
4. What are the challenges associated with the deployment of AI-driven malware detection and classification systems?

METHODOLOGY

This study adopts the meta-synthesis research design, which is a type of research that involves qualitative case studies of literature in a systematic approach to ascertain insights from available evidence in the literature (Leary & Walker, 2018). This approach is different from meta-analysis that does not provide comprehensive quality evidence on the data extracted from the literature. This study seeks to use provide insights on AI-driven malware detection and classification with a view of understanding the methods and effectiveness. The study is not limited to any geographical scope, which means that literature published anywhere globally are in consideration for selection. In a systematic literature review, process involves formulating research questions, searching relevant databases for literature, screening of literature with set inclusion and exclusion criteria, assessing the quality of the selected studies, extracting needed data from the studies using the rubrics of data extraction table, and analyzing the collected data based on the research questions (Lame, 2019).

This study conducted search on the literature by consulting different databases that may have relevant articles on AI-driven malware detection and classification with it a focus on its technique and effectiveness. Schut et al. (2024) recommended that credible and relevant databases should be considered in carrying out a systematic review. The databases consulted for this study include IEEE Xplore, Scopus, ACM Digital Library, Google Scholar, and Web of Science (See Table 2). These databases are considered to house relevant information material to answer the study's research question with the general aim of understanding AI-driven malware detection and classification. Series of relevant literature were search and retrieved after which some set inclusion and exclusion criteria were used to delimit the downloaded literature/articles. These criteria are presented in Table 1.

Table 1: Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
Primary research studies	Secondary research studies
Peer-reviewed studies	Non-peer reviewed studies
Studies published from 2015 to the present to ensure recent advancements	Studies published in 2014 or later
Articles focusing on AI-driven malware detection and classification	Articles that do not focus on AI-driven malware detection and classification
Quantitative, qualitative, and mixed-methods studies	Review

Source: Author's self-designed (2025)

Furthermore, the literature search was conducted using appropriate keywords and search terms. These search terms include "AI-driven malware detection", "AI-driven malware classification", "AI-driven malware detection technique", "AI-driven malware detection effectiveness", "AI-driven malware classification technique", and "AI-driven malware classification effectiveness". Moreover, synonymous words such as "methods" and "approaches" were used in place of "technique" in order to entrench the search results. The Boolean operators of "AND" and "OR" were used in the literature search. For instance, the search included search terms such as "AI-driven malware detection AND classification technique", "AI-driven malware detection OR classification technique", "AI-driven malware detection AND classification systems effectiveness", and "AI-driven malware detection OR classification systems effectiveness". Meanwhile, the Boolean "NOT" was not considered since it was not relevant in this study. Above all, the search strings were customized for each database to maximize relevant results.

Table 2: Electronic Search Strategy (Extracts for five databases)

S/N	Search terms	Web of Science	Scopus	Google Scholar	IEEE Xplore	ACM Digital Library
		Number of hits				
S1	AI-driven malware detection technique	1500	235	2000	672	506
S2	AI-driven malware detection classification	1300	180	1600	412	357
S3	AI-driven malware detection AND classification technique	3600	560	87200	4215	6019
S4	AI-driven malware detection OR classification technique	12000	8345	36000	3719	5417
S5	AI-driven malware detection AND classification systems effectiveness	9500	853	120000	5540	5178
S6	AI-driven malware detection OR classification systems effectiveness	8500	750	40000	2150	3500
Databases search limits adopted						
Duplicates removed		150	98	200	172	66
Titles and abstracts checked		100	72	120	114	40
Articles < or = 10 years (2015-2025)		25	18	22	24	08
Secondary research		12	09	08	12	04
Peer-reviewed articles/journals		05	12	06	05	04
English language only		NA	N/A	02	N/A	N/A
Final selected		3	6	3	1	2

Source: Author's Literature Search (2025)

Meanwhile, the Preferred Reporting for Systematic Reviews and Meta-Analyses (PRISMA) framework (see Figure 1) was used for structured data collection. This is believed to be the most popular and trustworthy framework for systematic reviews (Helach et al., 2023). Thus, it was considered for this study as the structured collection technique enhances objectivity, credibility, and repeatability. The 27-item PRISMA is divided into four categories, which include identification, screening, eligibility, and inclusion. The identification stage focuses on the literature search, which includes the sources and databases consulted for this study. These databases can be viewed in Table 2. The screening stage concerns the consideration of the title and abstracts of the retrieved literature from the consulted databases. The eligibility stage concerns the process of implementing the inclusion and exclusion criteria that have been outlined to consider the final selected literature. Having duly followed this process, the final selected literature for this study is thirteen (15).

European Journal of Computer Science and Information Technology, 13(52),13-33, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

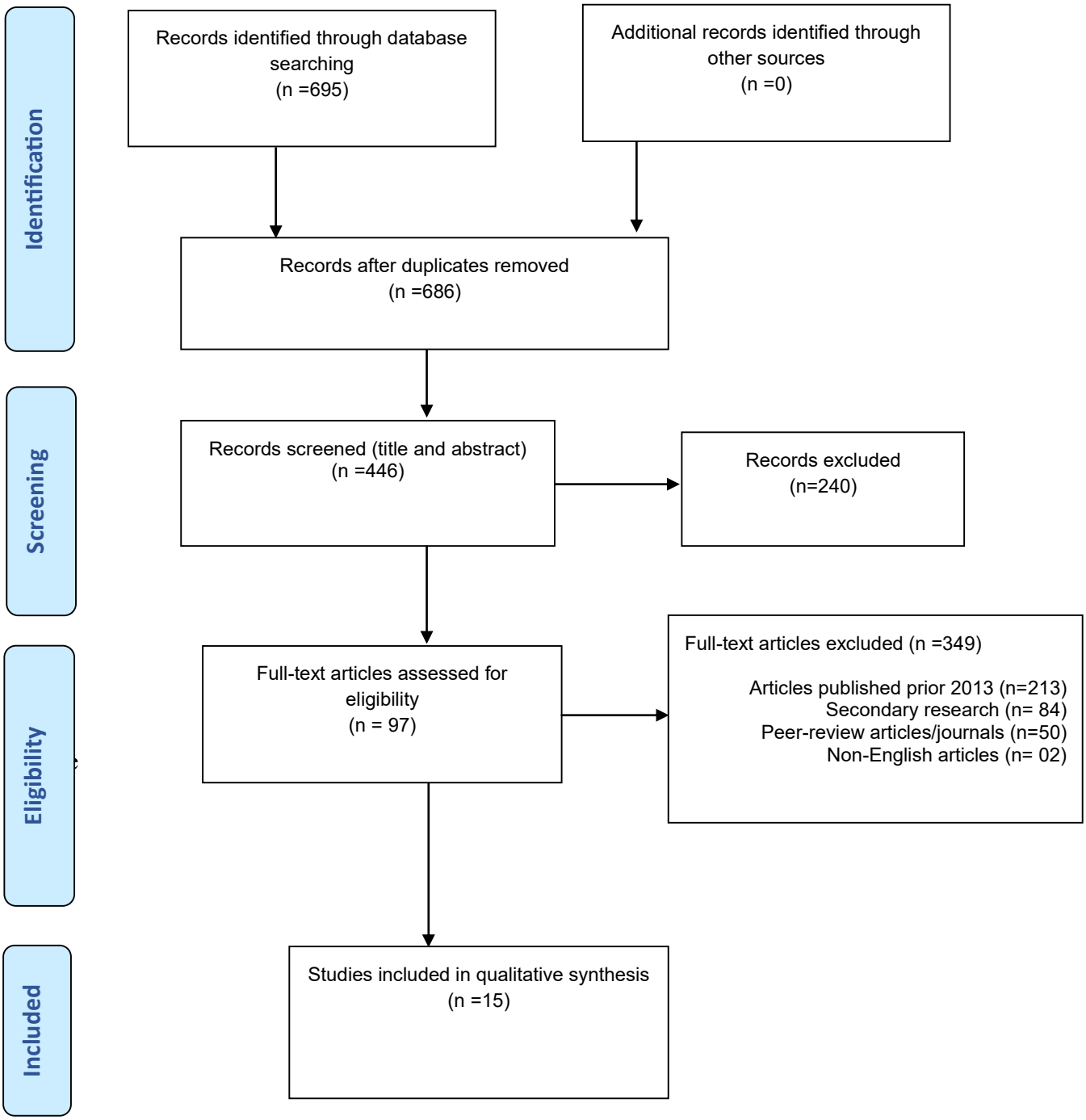

Figure 1: PRISMA diagram flow (Author's self-designed, 2025)

RESULTS AND DISCUSSION

As indicated in the PRISMA chart, the systematic review analyzed fifteen (15) studies, which focused on AI-driven malware detection and classification technique with specific focus on the techniques and classification. The selected studies span different sectors, which include healthcare, technology, retail, manufacturing, finance/business, transportation, and security ventures. This indicates that there is broad applicability of AI-enhanced malware defense systems. Moreover, the studies adopted different methodological approaches, which include datasets and experimental design. This offers diverse perspectives in understanding AI-enhanced malware detection and classification with a focus on its technique and effectiveness. The varying methodological approaches of the study suggests that the findings that emanate from this systematic review are deepened in varieties of ways to understand the phenomenon under study.

On the research question one, the results showed that the techniques used in AI-driven malware detection and classification include deep learning techniques, machine learning techniques, and hybrid models and emerging technologies. Deep learning techniques identified include generative adversarial networks (GANs) and autoencoders to improve predictive capabilities in malware detection systems (Almotiri, 2025), recurrent neural networks (RNN) and long short-term memory (LSTM) for network-based and memory-based malware detection (Bavadiya et al., 2025; Dash, 2024; Gopalsamy, 2023), convolutional neutral networks (CNN) for the extraction of complex spatial features malware samples (Dash, 2024; Manikandan et al., 2025; Mohammed et al., 2025), and graph neural networks (GNN) (Dash, 2024). The analytical methods and algorithm used for machine learning techniques include decision trees and random forests used for malware classification (Manikandan et al., 2025), extreme gradient and LightGBM used for malware detection in healthcare systems (Almotiri, 2025; Prabha et al., 2024), and naïve bayes (GNB) and linear discriminant analysis (LDA) employed for social media malware detection (Gopalsamy, 2023). Hybrid AI models (Bavadiya et al., 2025; Mohammed et al., 2025), explainable AI (Alohali et al., 2025; Prabha et al., 2024), and blockchain-integrated AI (Vekariya et al., 2025) are the hybrid model approaches identified in the final selected studies.

On the research question two, the findings revealed that AI-driven systems have high effectiveness in detecting and classifying malware, which indicates that relevance and usefulness. The results showed that two of the studies (Almotiri, 2025; Manikandan et al., 2025) demonstrated accuracy ranges of 97% to nearly 100% using Decision Trees and Random Forests. Moreover, it was shown that there is advanced deep learning, showing that CNN-based methods demonstrated superior performance in detecting complex malware patters (Dash, 2024; Mohammed et al., 2025). Bavadiya et al. (2025) demonstrated that AUC achieved high scores of 0.91-0.94 with the integration of autoencoders, random forests, and CNN-LSTM models. Moreover, two of the final selected studies (Alohali et al., 2025; Gopalsamy, 2023) demonstrated that real-time threat detection can be achieved through AI-driven systems with metrics such as recall, precision, and

F1-scores above 99%. Also, Phanireddy (2020) indicates that AI can detect obfuscated and polymorphic malware through de-obfuscation and adaptive learning.

On the research question three, results showed that there are different evaluation metrics and strategies in the final selected studies. The study demonstrated that there are standard metrics, benchmark datasets, experimental comparisons, and cross-validation and preprocessing. The studies showed that accuracy (Manikandan et al., 2025; Singh & Dubey, 2024); precision, recall, and F1 score (Almotiri, 2025; Dash, 2024; Gopalsamy, 2023); and area under curve (Bavadiya et al., 2025) are standard metrics for evaluating AI-driven malware detection and classification systems. The benchmark datasets used for evaluation include CIC-IDS2017, Microsoft Malware Dataset, EMBER, and BIG 2015 (Bavadiya et al., 2025; Gopalsamy, 2023; Polu, 2024). In terms of experimental comparisons, the AI-driven systems are often compared with traditional methods or the initial system to see the improvement with the introduction of the AI systems (Alohali et al., 2025; Prabha et al., 2024). Results showed that the use of cross-validation and preprocessing, feature selection, and class balancing techniques (Bavadiya et al., 2025; Singh & Dubey, 2024).

On the research question four, the challenges associated with the deployment of AI-driven malware detection and classification systems include dataset limitations (Mohammed et al., 2025; Bavadiya et al., 2025), computational complexity (Almotiri, 2025; Manikandan et al., 2025), interpretability (Alohali et al., 2025; Prabha et al., 2024), adversarial attacks (Dash, 2024; Phanireddy, 2020), and real-time deployment constraints (Gopalsamy, 2023; Singh & Dubey, 2024). All of these are challenges that are considered to be bottleneck in the use of AI-driven malware detection and classification systems. Thus, there is a need to ensure that all of these are given consideration towards the achievement of AI-enhanced systems for malware detection and classification.

CONCLUSION

The study concludes that AI-driven malware detection and classification spans across different fields. It was established that there are different techniques used in AI-driven malware detection and classification. These techniques can help increase predictive capabilities in malware detection systems, which can be used for malware detection and classification. Despite the several challenges associated with the use of AI-driven malware detection and classification, the study recognized that AI-driven malware detection and classification are highly effective compared to traditional methods or the methods that are available at the moment. This emphasizes the relevance and usefulness of AI-enhanced systems for malware detection and classification. The study established that there are different evaluation strategies of AI-driven malware detection and classification, which include standard metrics, benchmarked datasets, experimental comparisons, and cross-validation. The study established that the challenges associated with the use of AI-driven malware detection and classification systems include dataset limitations, computational complexity, adversarial attacks, interpretability, and real-time deployment constraints.

Implications

The study provides policy and practical implications. Government and regulatory bodies should incorporate AI-driven malware detection and classification within their different countries' cybersecurity frameworks. They should come up with policies and mandate the integration of AI-driven solutions in sectors such as national security, health, and finance. Also, governments should prioritize the funding of research that seeks to provide more evidence on AI-driven cybersecurity solutions to address challenges such as interpretability, dataset limitations, and adversarial attacks. Moreover, there is a need for policymakers in different countries to design policies that will encourage secured and ethical data sharing among cybersecurity experts to overcome the challenge of dataset limitations. This will improve the robustness of the available datasets and enhance AI-driven malware detection and classification.

The study will be of benefit to cybersecurity experts and practitioners as it will provide them with evidence on how they can enhance cyber defense with the integration of AI-driven tools into their security operations to improve malware detection and classification. The study will be relevant to experts to help them optimize the available security resources using predictive AI tools to improve operational efficiency. Moreover, organizations and developments should consider the application of standardized evaluation strategies to validate and improve their AI models before or after deployment in malware detection and classification. Furthermore, developers should address challenges like computational complexity and real-time constraint if they want to have AI-driven systems that are practical for real-world use. Moreover, there is a need for cybersecurity experts to be resilient against advanced threats by ensuring that their model robustness is improved to forestall adversarial attacks.

Recommendations

The following recommendations are proffered based on the study's findings:

1. There is a need for continuous update of datasets to reflect new attack vectors.
2. Organizations and cybersecurity experts should adopt AI-enhanced malware detection and classification systems to enhance efficiency and effectiveness.
3. There is a need for more awareness on the need for a pool or cloud for datasets to enhance datasets sharing, which can address the challenge of dataset limitations.
4. It is recommended that developers should consider the use of explainable AI (XAI) to improve interpretability of AI-based malware detection and classification systems.
5. There is a need for cybersecurity expert to incorporate adversarial defense mechanisms.

REFERENCES

Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-Rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. *Applied Sciences*, *12*(17), 8482.

Abusitta, A., Li, M. Q., & Fung, B. C. (2021). Malware classification and composition analysis: A survey of recent developments. *Journal of Information Security and Applications*, *59*, 102828.

Almotiri, S. H. (2025). AI driven IOMT security framework for advanced malware and ransomware detection in SDN. *Journal of Cloud Computing*, *14*(1), 1-19.

Alohali, M. A., Alahmari, S., Aljebreen, M., Asiri, M. M., Miled, A. B., Albouq, S. S., ... & Alqazzaz, A. (2025). Two stage malware detection model in internet of vehicles (IoV) using deep learning-based explainable artificial intelligence with optimization algorithms. *Scientific Reports*, *15*(1), 20615.

Anderson, H. S., Kharkar, A., Filar, B., & Roth, P. (2017). Evading machine learning malware detection. *Black Hat*, *2017*, 1-6.

Arivudainambi, D., KA, V. K., & Visu, P. (2019). Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance. *Computer Communications*, *147*, 50-57.

Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE Access*, *8*, 6249-6271.

Aslan, Ö., & Yilmaz, A. A. (2021). A new malware classification framework based on deep learning algorithms. *IEEE Access*, *9*, 87936-87951.

Bavadiya, P., Upadhyaya, P., Bhosle, A. C., Gupta, S., & Gupta, N. (2025). AI-driven data analytics for cyber threat intelligence and anomaly detection. In *2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 677-681). IEEE.

Cakir, B., & Dogdu, E. (2018). Malware classification using deep learning methods. In *Proceedings of the 2018 ACM Southeast Conference* (pp. 1-5).

Chanajitt, R., Pfahringer, B., & Gomes, H. M. (2021). Combining static and dynamic analysis to improve machine learning-based malware classification. In *2021 IEEE 8th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 1-10). IEEE.

Chandran, S., Syam, S. R., Sankaran, S., Pandey, T., & Achuthan, K. (2025). From static to ai-driven detection: A comprehensive review of obfuscated malware techniques. *IEEE Access*.

Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., & Stamp, M. (2017). A comparison of static, dynamic, and hybrid analysis for malware detection. *Journal of Computer Virology and Hacking Techniques*, *13*, 1-12.

Dash, C. S. (2024). AI-driven defense mechanisms for protecting industry 5.0 from android malware threats. In *2024 International Conference on Communication, Computing and Energy Efficient Technologies (I3CEET)* (pp. 1735-1740). IEEE.

Deldar, F., & Abadi, M. (2023). Deep learning for zero-day malware detection and classification: A survey. *ACM Computing Surveys*, *56*(2), 1-37.

Faiz, A., Jumani, A., Hafiz, A., Shujah, S., Talpur, M. R. H., & Majid, A. (2025). Enhancing Cybersecurity Through AI: A Machine Learning-Based Framework for Real-Time Threat Detection and Mitigation. *Annual Methodological Archive Research Review*, *3*(6), 48-71.

Gopalsamy, M. (2023). AI-driven solutions for detecting and mitigating cyber threats on social media networks. *International Journal of Advanced Research in Science, Communication and Technology*, *3*(2), 692-702.

Helach, J., Hoffmann, F., Pieper, D., & Allers, K. (2023). Reporting according to the preferred reporting items for systematic reviews and meta-analyses for abstracts (PRISMA-A) depends on abstract length. *Journal of Clinical Epidemiology*, *154*, 167-177.

Hsieh, W. C., Wu, C. C., & Kao, Y. W. (2015). A study of android malware detection technology evolution. In *2015 International Carnahan Conference on Security Technology (ICCST)* (pp. 135-140). IEEE.

Islam, R., Tian, R., Batten, L. M., & Versteeg, S. (2013). Classification of malware based on integrated static and dynamic features. *Journal of Network and Computer Applications*, *36*(2), 646-656.

Kalash, M., Rochan, M., Mohammed, N., Bruce, N. D., Wang, Y., & Iqbal, F. (2018). Malware classification with deep convolutional neural networks. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE.

Lame, G. (2019). Systematic literature reviews: An introduction. In *Proceedings of the design society: international conference on engineering design* (Vol. 1, No. 1, pp. 1633-1642). Cambridge University Press.

Leary, H., & Walker, A. (2018). Meta-analysis and meta-synthesis methodologies: Rigorously piecing together research. *TechTrends*, *62*(5), 525-534.

Liu, K., Xu, S., Xu, G., Zhang, M., Sun, D., & Liu, H. (2020). A review of android malware detection approaches based on machine learning. *IEEE Access*, *8*, 124579-124607.

Maddireddy, B. R., & Maddireddy, B. R. (2023). Automating malware detection: A study on the efficacy of AI-driven solutions. *Journal Environmental Sciences and Technology*, *2*(2), 111-124.

Manikandan, K. P., Onteddu, N. R., & Chilimi, A. K. (2025). Next-gen malware detection using ai ai-powered malware threat detection automated malware classification through machine learning. In *2025 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 581-588). IEEE.

McLaughlin, N., Martinez del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., ... & Joon Ahn, G. (2017). Deep android malware detection. In *Proceedings of the seventh ACM on conference on data and application security and privacy* (pp. 301-308).

Moamin, S. A., Abdulhameed, M. K., Al-Amri, R. M., Radhi, A. D., Naser, R. K., & Pheng, L. G. (2025). Artificial intelligence in malware and network intrusion detection: A comprehensive

survey of techniques, datasets, challenges, and future directions. *Babylonian Journal of Artificial Intelligence*, *2025*, 77-98.

Mohammed, S., Sultana, G., Aasimuddin, F. M., & Chittoju, S. S. R. (2025). AI-driven automated malware analysis. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, *13*(1), 23-29.

Pascanu, R., Stokes, J. W., Sanossian, H., Marinescu, M., & Thomas, A. (2015). Malware classification with recurrent networks. In *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (pp. 1916-1920). IEEE.

Phanireddy, S. (2020). AI generated malware detection in web applications de-obfuscation and analysis. *International Journal of Leading Research Publication*, *1*(4), 1-9.

Polu, O. R. (2024). AI-driven malware classification using static and dynamic analysis. *International Journal of Science and Research*, *13*(6),

Prabha, M., Hossain, M. A., Samiun, M., Saleh, M. A., Dhar, S. R., & Al Mahmud, M. A. (2024). AI-driven cyber threat detection: Revolutionizing security frameworks in management information systems. In *2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)* (pp. 357-362). IEEE.

Rao, V., & Hande, K. (2017). A comparative study of static, dynamic and hybrid analysis techniques for android malware detection. *International Journal of Engineering Development and Research*, *5*(2), 1433-1436.

Schut, M., Adeyemi, I., Kumpf, B., Proud, E., Dror, I., Barrett, C. B., ... & Leeuwis, C. (2024). Innovation portfolio management for the public non-profit research and development sector: What can we learn from the private sector? *Innovation and Development*, 1-19.

Singh, A., & Dubey, S. K. (2024). Revolutionizing malware detection techniques by using predictive AI. In *2024 International Conference on Computing, Sciences and Communications (ICCSC)* (pp. 1-6). IEEE.

Tahir, R. (2018). A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, *8*(2), 20-31.

Vekariya, D., Vasani, H., Patel, A., Jadhav, R., Soni, R., & Kumar, M. (2025). AI driven malware detection using blockchain. In *IET Conference Proceedings CP920* (Vol. 2025, No. 7, pp. 261-267). Stevenage, UK: The Institution of Engineering and Technology.

Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, *50*(3), 1-40.

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

APPENDIX I
DATA EXTRACTION TOOL
AI-Driven Malware Detection and Classification: A Systematic Review of Techniques and Effectiveness

S/N	Research titles and authors	Industry/Organisation	Methodology	Findings
1	Next-gen malware detection using AI AI-powered malware threat detection automated malware classification through machine learning Manikandan et al. (2025)	Retail	The models are evaluated on a dataset comprising 100,000 samples with 35 system-level behavioral features. Experimental results indicate that Decision Tree, Random Forest, and KNN achieve nearly 100% accuracy, significantly outperforming conventional compact data-based methods.	- CNN achieves 97.79% accuracy, showcasing deep learning's potential, whereas SVM attains 86% accuracy but demands higher computational resources.
2	Automating malware detection: A study on the efficacy of AI-driven solutions Maddireddy and Maddireddy (2023)	Healthcare	Drawing upon a diverse dataset of malware samples spanning various families and characteristics, the study employed state-of-the-art machine learning algorithms to develop and evaluate AI-driven malware detection models. This approach leverages advanced feature extraction techniques, including static and dynamic analysis, to capture nuanced patterns and behaviors indicative of malicious intent.	- The results of the study demonstrate the superiority of AI-driven solutions in automating malware detection compared to traditional methods. The models achieve high detection rates with low false positive rates, indicating their robustness and reliability in identifying malicious software accurately. Furthermore, the adaptability of the models to evolving malware landscapes enables proactive threat mitigation and enhances the resilience of cybersecurity defenses.

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

3	AI-driven automated malware analysis. Mohammed et al. (2025)	Manufacturing	The study tests both conventional machine learning algorithms and state-of-the-art deep learning models. The study also points to the necessity of balanced datasets and hybrid analysis methods, which apply both static and dynamic techniques for dealing with malware complexity.	- Results showed that AI-driven approaches for automated malware analysis represent great progress in the field of cybersecurity. Through these approaches, machine learning and deep learning models have been proven to establish good detection and classification accuracy of malware strains. The study has shown that the use of deep learning techniques, in particular CNN, offers a better approach in identifying complex patterns and adapting to changing threats. - Experimental results underscore the need for balanced and diversified datasets, robust feature engineering, and hybrid approaches that use static and dynamic analysis.
4	AI driven IOMT security framework for advanced malware and ransomware detection in SDN Almotiri (2025)	Healthcare	The study designed a system to tackle rising Software Defined Network (SDN) security threats especially in healthcare environment to the risk of malware, and ransomware attacks, is powered by Deep Learning (DL) and Machine Learning (ML) technologies to work together, as a static and dynamic scanning methods.	- The double tier eXtreme Gradient Boosting (XGBoost) performance reaches 99.60% accuracy with an F1 score of 0.9966 and outperforming the benchmark model at 98.80% accuracy and F1 score 0.988. Further, a two-layer Light Gradient Boosting Machine (LightGBM) model achieves 99.32% accuracy with an F1 score of 0.9934, in contrast to which at 98.96% accuracy and an F1 score of

			Using this, execution traces and the Application Programming Interface (API) call sequences are integrated with Generative Adversarial Networks (GANs) and autoencoder based predictive analysis to improve the threat detection.	0.9895, beats its benchmark counterpart. Furthermore, the Deep Neural Network (DNN) system with bi layered also achieves 99.13% accuracy and F1 score of 0.9915.
5	AI generated malware detection in web applications de-obfuscation and analysis Phanireddy (2020)	Technology	Gather both malicious web scripts (from honeypots, threat intelligence feeds) and legitimate code repositories (e.g., open-source libraries).	- Results showed that AI-generated malware poses a formidable challenge to web application security, leveraging obfuscation, polymorphism, and even adversarial techniques to bypass traditional defenses. By combining dynamic and static analysis with machine learning classifiers, defenders can identify malicious scripts regardless of how many times they have been repacked or altered. Deobfuscation further enhances these efforts, revealing hidden logic that might otherwise remain unseen.
6	AI driven malware detection using blockchain Vekariya et al. (2025)	Technology	The study adopted a system using artificial intelligence in conjunction with blockchain technology and Docker-based containerization designed to improve on the malware detection.	- The study shows that the innovative methods do not only enhance the capacity for threat detection but also guarantee data security via the powerful encryption provided by the blockchain. The system is very much reliable and flexible against the continuously

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

				changing cyber threats, thus towards a secure digital environment through integration of AI, blockchain, and containerization.
7	Artificial intelligence in malware and network intrusion detection: A comprehensive survey of techniques, datasets, challenges, and future directions Moamin et al. (2025)	Finance	Static, dynamic, and hybrid analysis techniques are compared, with a focus on feature engineering, behavioral modeling, and real-world deployment constraints. A novel AI-based Malware Detection and Prevention Framework is proposed, combining machine learning classifiers with Network Intrusion Prevention Systems (NIPS) to enhance proactive defense capabilities.	- Prominent AI methods such as decision trees, Bayesian networks, deep learning, fuzzy logic, support vector machines, and genetic algorithms have been applied to malware detection, each offering unique strengths in handling specific threat models. - The study proposed a hybrid AI malware detection and prevention framework combining AI-based malware classifiers and network intrusion prevention systems (NIPS).
8	AI-driven data analytics for cyber threat intelligence and anomaly detection Bavadiya et al. (2025)	Technology	The study presents a novel hybrid AI-based data analysis framework for cyber threat intelligence and anomaly detection. It proposed a model that combines autoencoders, random forests, and CNN-LSTM architectures to improve anomaly detection and classification. The dataset used for training and evaluation is the	- The AE-RF module learns the normal behavior of the system to detect abnormal behavior, and the CNN-LSTM model identifies spatial and temporal properties of malware for execution patterns. This article ensures that the dataset is well-preprocessed, including feature extraction, PCA, and SMOTE for class balancing to provide optimal model performance. - The experimental results show that AE-RF has an area under curve

			Microsoft Malware Dataset, a publicly available dataset.	(AUC) score of 0.91 and CNN-LSTM has 0.94, which demonstrates that unsupervised and supervised techniques together have high classification accuracy. This hybrid approach not only improves malware detection accuracy but also enhances cyber threat intelligence by providing interpretable insights into attack patterns.
9	AI-driven solutions for detecting and mitigating cyber threats on social media networks Gopalsamy (2023)	Business	Leveraging the CIC-IDS2017 dataset. Data using text-based features, like user behaviour and network activity, are then preprocessed and feature-engineered, for instance, by means of one-hot encoding. Classification models such as LSTM, GNB, and LDA were used to group various cyber hazards, such as malware propagation, into distinct groups.	- Thus, the LSTM reveals its high potential in real-time threat identification in terms of an accuracy of 99.34%, recall of 99%, precision of 99.3%, and an F1-score of 99.34%. However, it reveals that GNB and LDA have lower accuracy and classification measures compared to other algorithms.
10	Two stage malware detection model in internet of vehicles (IoV) using deep learning-based explainable artificial intelligence with optimization algorithms Alohali et al. (2025)	Transportation	The study proposed a novel Malware Detection Model in the Internet of Vehicles Using Deep Learning-Based Explainable Artificial Intelligence (MDMIoVDLXAI). Initially, the data normalization stage is	- The results showed that the MDMIoV-DLXAI methodology achieves better ROC results over each class, indicating its essential capacity for discerning class labels. This trustworthy tendency of maximum ROC analysis across multiple classes shows

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

			performed by the min-max normalization to convert input data into a beneficial format. Besides, the proposed MDMIoV-DLXAI model utilizes the reptile search algorithm (RSA) model for feature selection. Furthermore, the hybrid of bidirectional long short-term memory with a multihead self-attention (BiLSTM-MHSA) model is employed for the malware classification process.	the capable outcomes of the MDMIoV-DLXAI technique on forecasting class labels. - The experimental evaluation of the MDMIoV-DLXAI method is examined under the malware dataset. The comparison study of the MDMIoV-DLXAI method demonstrated a superior accuracy value of 97,393% over existing techniques.
11	AI-driven defense mechanisms for protecting industry 5.0 from android malware threats Dash (2024)	Technology	This study seeks to establish the level of accuracy of CNN, RNN, and GNN in the classification of Android malware threats in industrial 5. 0 applications. To notice the strengths and weaknesses of these neural network architectures the following evaluation metrics are used: precision, recall, F1-score, and accuracy.	- From the obtained results, it is seen that though CNNs provide fairly good accuracy and recall and log loss in most of the cases, RNNs succeed in sequential data analysis, and GNNs are significantly higher in precision and accuracy in case with graph data. - The study reveals the applicability of GNNs to the tasks that call for fine-grained analysis of relations and high detection accuracy of malware.
12	Malware traffic classification using principal component analysis and artificial neural	Security venture	The study proposed robust traffic classification system using Principal Component	- Experimental results confirm that the proposed schemes are efficient to classify the attack traffic with 99% of

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

	network for extreme surveillance Arivudainambi et al. (2019)		Analysis (PCA) and Artificial Neural Network (ANN) for providing extreme surveillance	accuracy when compared to the state-of-the-art methods.
13	AI-driven cyber threat detection: Revolutionizing security frameworks in management information systems Prabha et al. (2024)	Technology	Multiple machine learning models are evaluated, including XGBoost, Random Forest, Support Vector Machines (SVM), and K Nearest Neighbors (KNN).	- XGBoost achieved a near-perfect accuracy of 99.99% on these, and so might be able to classify these as they do cyber threats accurately. This proposed framework combines PCA and LIME in a new configuration specifically suited for real-time MIS applications: this makes it possible to achieve both high accuracy and interpretability in the face of various attack types using the CICIDS 2017 dataset. - Considering interpretability, this analysis emphasizes cybersecurity in which transparent decision-making models allow professionals to understand, validate, and respond convincingly to detected anomalies.
14	AI-driven malware classification using static and dynamic analysis Polu (2024)	Business	Publicly available and enterprise malware repositories (EMBER (static analysis), CIC - MalMem (memory dumpbased classification) and BIG 2015 (behavioral analysis dataset) form the dataset used for this study. Benign and malicious	- The result feature set obtained using proposed approach is robust feature set that harness static features (opcode sequences, API calls) and dynamic behavioral patterns (system calls, memory dumps, network activity). - The accuracy and robustness are improved by comparison on benchmark

Print ISSN: 2054-0957 (Print)

Online ISSN: 2054-0965 (Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development -UK

			samples of ransomware, trojans, worms, spyware, APTs, etc. make up the dataset.	datasets (EMBER, CIC - MalMem, BIG 2015).
15	Revolutionizing malware detection techniques by using predictive AI Singh and Dubey (2024)	Technology	The study developed and implemented AI-enabled Threat Intelligence (AI-TI) systems, with a focus on Random Forest, K-Nearest Neighbors (KNN), and XGBoost. The study methodology encompasses a multifaceted approach, beginning with the collection and preprocessing of extensive datasets comprising internal network logs, security incident reports, and open-source threat intelligence feeds.	- Through empirical experimentation and performance evaluation, the efficacy of each algorithm in detecting and mitigating cyber threats is rigorously assessed. - Key performance metrics such as detection accuracy, false positive rates, and response times are analyzed to ascertain the optimal configuration and deployment strategy for AI-TI systems. By harnessing the capabilities of Random Forest, KNN, and XGBoost algorithms, organizations can enhance their cyber resilience and effectively combat the evolving threat landscape.