Journal of Engineering Research and Education
Volume 18, (Special Issue) 2026 [109-118]

AI-Powered and Conventional Malware Detection Approaches: Challenges and Future Trends

Eyman F. A. Elsmany[1,*], Zeinab E. Ahmed[1], Aisha A Hassan[2], Altahir A. Altahir[3],
and Mohammed S. Elbasheir[4]

[1]Department of Computer Engineering, University of Gezira, Sudan
[2]Department of Electrical and Computer Engineering, International Islamic University Malaysia (IIUM), Gombak, Malaysia.
[3]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman (UTAR), Malaysia
[4]School of Electronics Engineering, Faculty of Engineering, Sudan University of Science and Technology, Khartoum, Sudan

ABSTRACT

The continuous increase in users on the internet and online services provisioning such as shopping and banking causes many cyber criminals with a massive number of hackers sniffing users' data. Malware is increasingly evolving, and the growth of worms, viruses, spyware, trojan horses, and other developments of malicious code requires improved detection techniques which are directed to the use of dynamic malware detection techniques. As a result, there is a growing need for anti-malware methods for protection of internet users' privacy. Conventional mechanisms, such as behavior-based and signature-based approaches, have been broadly used but face great challenges compared to the growing malware threats. Artificial Intelligence AI-driven methods, leveraging Deep Learning (DL) and Machine Learning (ML), offer better adaptability and detection rates. This article serves as a survey, which investigates conventional and AI-powered malware detection techniques. Also, it offers a comparative analysis model, such as adaptability, accuracy, scalability, resource requirements, cost and more to signal their strengths and weaknesses. Finally, the study highlights future developments to mitigate the limitations of both approaches and improve overall cybersecurity resilience.

Keywords: Malware, cybersecurity, Artificial Intelligence, Machine Learning, Deep Learning

1. INTRODUCTION

In the current era, the internet services and applications have become crucial for nearly everyone in society part of daily life. The usage of the internet has expanded from social interactions and online banking to marketing and health-related transactions. It is nearly impossible to function effectively without access to the internet. However, as the internet continues to develop, criminals have transferred their focus from the physical realm to the digital world. Malicious software, labelled as malware, are initiated to attack systems' security and generate illegitimate revenues [1]. Their illegal actions comprise identity theft and data violations, and able to spread out through various computers, systems or software applications [2]. Cybercriminals repeatedly use malicious software, or malware, to carry out attacks on their target devices and have widely used malware to intentionally exploit or harm desktop, smartphones, IoT, vehicle platforms or other systems. Malware can takes several forms, like worms, rootkits, trojan horses, ransomware, and viruses [2]–[4]. Each type of malware is created to achieve specific goals, whether it's enabling remote control, damaging systems, stealing sensitive information, or other risky actions.

[*]eymanelsmany@gmail.com

Hacker cyberattacks are the leading cause of complexity of cyber threats. These attacks are on the rise, necessitating advanced detection methods. Traditional malware detection relies on known signatures and behaviour rules. Identify malware using file or signatures, while behaviour-based approaches detect malware by analysing suspicious actions during execution [5]. Conventional malware was typically designed for straightforward, often consisting of a single process without complex hiding mechanisms. However, traditional detection methods have proven ineffective against newer generations of worms, viruses, spyware, trojan horses, and other advanced malicious codes with sophisticated obfuscation strategies. With recent advancements in artificial intelligence (AI) technology, AI-driven techniques leveraging DL and ML are now being employed to analyse patterns and provide real-time 24/7 dynamic defence mechanisms [6].

DL and ML detection methods can identify both known and unknown malware. Malware detection relies on various AI models, with neural networks growing increasingly complex over time. AI models are broadly classified into two categories: shallow learning and deep learning. These models utilize multiple learning approaches, including supervised, unsupervised, semi-supervised, and self-supervised methodologies. In the beginning stages of AI, the supervised learning method applying shallow model primarily. However, the necessity of deep learning has emerged duo to handle large datasets, inaccurate labels and imbalanced datasets [7]. Since each AI model has diverse features, based on the purpose of using the AI model has been chosen. Many studies determined and showed the AI effectiveness in malware exposure but still no technique could expose all new generation and sophisticated malware. This paper investigates conventional and AI- powered malware detection approaches and open potential hybrid solutions. Also analyses their strengths and weaknesses in terms of adaptability, accuracy, resource requirements, cost, scalability and more. Finally, the study highlights future developments to mitigate the limitations of both approaches and improve overall cybersecurity resilience. The remainder of the article is structured as follows: Section II studies malware analysis tools and Section III offer malware detection approaches. Section IV provides a comparative analysis of conventional and AI-powered malware detection methods. Section V discusses open issues and future research trends. Section VI, concludes the research and defines future works.

2. MALWARE ANALYSIS APPROACHES

Malicious software poses a major threat to privacy, system integrity, and data security. Malware samples are analyzed to identify features for detection. Consequently, the process of investigating malicious software to recognize its behavior, impact and functionality is known as malware analysis. In this section, various approaches to malware analysis are described. It is an essential step in developing effective detection and mitigation schemes. Malware analysis is mainly characterised into two core forms: dynamic and static analysis.

2.1 Static Analysis (SA)

This type involves assessing the source code of the suspicious software without executing the file under investigation. The procedures include disassembling, decompiling, and analyzing binary files. SA is effective for identifying signatures and recognizing the malware's structure but may struggle with packed malware or obfuscated [8]. Through SA various static data types can be collected, including portable executable (PE) data header [4], developed data such as compression ratio and string-based entropy. Furthermore, SA tools, such as Python-developed modules and IDA pro disassembler, are utilised to gather static operational code (opcode) and Application Programming Interface (API) calls [3]. Although SA can trace all the potential execution path, it is prompted by encryption and packing procedures. Such as PeStudio, Ghidra, Capstone, Binwalk, and IDR which are used to analyze binaries or files without running them.

2.2 Dynamic Analysis (DA)

It concerns running the malware in an inaccessible environment as a sandbox to monitor its behaviour. DA is effective for discovering unknown or obfuscated malware simply requires a secure setup to avoid unintended damage. Several DA tactics have been used to gather various data types to distinguish between benign files and malware via configure executable files in controlled environment, emulators or virtual machine (VMs) to observe the configurable file behavior at runtime and collect linked dynamic data. Applying a dynamic scheme may offer benefits over classifying malware as compared to static methods. This is because, unlike static tools, identifying dangerous behaviours during execution is significantly more complex [9]. Dynamic tools such as Process Hacker, Process Monitor (ProcMon), Fiddler, Wireshark, and Cuckoo Sandbox monitor or interact with live system activities [6]. Although complicated malware usually unable conceal how it acts and perform when analysed dynamically. Although DA cannot assure all malware cases to investigate execution path [5]. Table 2 presents a comparison of static and DA tools.

3. DETECTION APPROACHES for MALWARE

Malware detection is the most significant mechanism of cybersecurity. Malware detection tools run continuously and gather automated updates with reference information to recognize malicious code. Malware detection mechanisms are primarily categorized into two main types: conventional and AI-powered methods.

3.1 Conventional Malware Detection Approaches

The majority conventional strategies for finding malware use signature-based detection. This means that a system compares the characteristics of a file to a known database of malware signatures to find malicious software, that utilized a lot by most antivirus programs [10]. Other traditional methods include basic behavioural monitoring, which analyses behaviour patterns and file content to detect possible threats. However, they may have weaknesses against new or expanding malware.

Signature-Based Detections: Signatures are a malware characteristic that encapsulates the system structure and uniquely labels every malware case. Patterns include file code snippets, byte sequences, or file hashes. The procedure of signatures-based malware detections mostly relies on the creation of a signatures database; this database is systematically updated as new malware variants develop [11]. Consequently, when a program or file is examined, the detection system breaks it down into smaller components and matches its content to recognized malware signatures database. If a correspond is found, the file is identified as unsafe, and appropriate actions to be taken such as deleting, quarantining or repairing mechanisms.

This technique is highly effective against common threats and offers efficiency, ease of implementation, and a low false alarm rate [21]. Despite being a foundational cybersecurity measure, it struggles with zero-day and polymorphic malware attacks. Where malware fluctuates its code or structure with every infection while maintaining its functionality, while signature-based detection dependence on pre-existing signatures causes it to be less effective against new and developing malware. In 2017, Jing, Li et. al. [22] evaluated signature-based detection for network threats. It considers the principles, implementation steps, strengths, limits, and potential upgrades of this detection method. Signature-based detection is reliable but unsuccessful against advancing cyber threats such as polymorphic and zero-day attacks. Additionally, researchers [23] have presented a methodology to improve signature-based intrusion detection systems (IDS) by advancing database efficiency and detection speed. Decreasing signature database size enhances effectiveness with no compromising accuracy. In 2019, another study [24] investigated signature-based techniques in antivirus produce, assessing their efficiency, trade-offs, performance and detection algorithms. So, Signature-based detection yet essential but demands hybrid approaches to fighting modern threats.

Table 2 Comparison of SA and DA tools

Tools	Analysis Type	Use Case	Key Features	Limits
PeStudio [12]	SA	Early triage of PE files	User- friendly and lightweight	Cannot discover runtime activities and restricted to static analysis
Ghidra [13]	SA/ DA	Inverse engineering	Open source Cross-platform Supports scripting	Steep learning curve
IDA Pro [3]	SA/ DA	Complex reverse engineering	Powerful disassembly and de-compilation	Complex for beginners Expensive
Binwalk [14]	SA	Embedded file or firmware analysis	Extracts embedded files	Excluding effective for non-firmware files Restricted to static analysis
Capstone [15]	SA	Dismantling framework for property developer	Supports multiple architectures lightweight Proposes a consistent API across various platforms	Not a standalone tool
IDR [16]	SA	Analysis of Delphi binary	Easy to use Offers an interactive interface for discovery	Restricted to Delphi files
Process Hacker [17]	DA	System monitoring and process	Real-time process check Open source	Restricted to runtime analysis and no static analysis expertise
ProcMon [18]	DA	Monitoring of System activity	Describes full system activity logs Real-time monitoring	No static analysis expertise and overwhelming data output
Fiddler [6]	DA	Assessment of web traffic	Easy to use Informative for analyzing malware interaction over HTTP/HTTPS	Restricted to web traffic and needs manual configuration
Cuckoo Sandbox [20]	DA	Automated analysis of malware	Completed behavioral reports and supports insights into possible effects of malware	Resource-exhaustive Needs set-up and maintenance

Abbas, M.F.B et. al. In [25] explored the challenge of malware detection in IoT devices using signature-based procedures. It requires big signature databases, which create extreme resources overhead. Consequently, due to high storage and processing demands, signature-based detection is ineffective for IoT devices. In [26] Hardware-Level Malware Detection (HLMD) extracts interactive signatures as of hardware events. Thus, hardware-assisted malware detection is a promising alternative to usual signature-based and behaviour-based methods.

Behaviour-Based Detections: In this approach, the malware detection is achieved and constructed to its behaviour. A behaviour-based method is utilised to mitigate the signature-based technique restrictions. The primary improvement of these techniques is that zero per day malicious could be identified. But the main difficulty of these techniques that it could result extreme false alarms if all malware scenarios are not well investigated. In 2020, M. G. R. Scholar and R. Kumar [11] discussed the signatures-based and behaviour-based malicious detections pipeline process. It justifies how both methods work, their advantages, and their constraints. Therefore, for detecting the new and evolving malware threats the behavior-based detection is more efficient. In 2022, [27] proposed a method combines statistical filtering with a composite autoencoder (CAE) which is behaviour-based methods to detect anomalies in industrial control systems (ICS).

Hence, the hybrid method reduces false negatives while having excluding detection time. M. A. Galal et. al. in [28] highlighted the challenges of malware different detection appointed to code obfuscation techniques such as metamorphism and polymorphism, which avoid signature-based detection. However, behaviour-based detection continues effective because malware modifications share similar behaviours, particularly in their use of API calls for performing malicious duties. In 2018, [29] established normal user behaviour profiles and comparing observed actions against these profiles that to detects questionable activities. Subsequently, outcome a high detection accuracy and eliminating duplicate records in the dataset. The study in [30] examined the developments in behaviour-based Intrusion Detection Systems (IDS), their powers, limitations, and improvements. Accordingly, behaviour-based IDS is further efficient against unspecified attacks.

3.2 Powered Malware Detection

Previously, the malware attacks were particularly low, and elementary detection tools such as manual identified through pre-execution filter rule where appropriate to distinguish most malware types. However, as malwares becomes farther complex and sophisticated, conventional detection methods frequently fail, needing, necessitating advanced techniques and tools [4]. In a dynamic analysis situation, evasive malware can utilize differed anti-analysis procedures to detect the environment in which it is functioning, and then to behave inversely and hide its evil intent if it detects it is under analysis [31]. AI is a broad term for several ML and DL systems.

Machine Learning-Based Detection: Supervised and unsupervised learning models are utilised to analyze static and dynamic features of files. Regular model updates and labelled training data are essential. These models can recognize patterns from sizable data sets to detect malware and can distinguish zero-day malware based on behaviour patterns. To address the restrictions of signature-based detection in recognizing unknown malware and finding new variants variants in [32] suggested a system consists of data processing, decision-making, and new malware detection modules. It presented 98.9% classification accuracy explaining the effectiveness of ML-based detection over signature-based methods. The article [33] evaluates adversarial attack methods, protecting techniques and the restrictions of presented intrusion detection datasets. The findings denote that adversarial attacks significantly weaken ML-based security systems, although existing defines mechanisms are still lacking and demand further upgrading. In 2023, [34] surveyed the evolution of malware classification in the framework of ML-based detections and attacks.

ML models are exposed to evasion Attacks. Hence, attackers manipulate malware aspects such as byte sequences, API calls to trick classifiers. K. Aryal et. al. [35] conducted a study that classifies adversarial attack procedures, evaluates their impact on malicious classifiers, and offered a categorization of adversarial evasion attacks across Android, Windows, and PDF malware detection models. Additionally, it highlighted how attackers manipulate malware patterns to avoid detection by ML-based security techniques. ML-Based malware exposure is vulnerable to adversarial attacks. Where the attackers modulate small portions of malware to evade classifiers without stopping functionality. In 2021, [21] afforded a broad study on ML-based malwares detection in configurable files. SVM, Random Forest (RF), Decision Trees (DTs), and DL models are broadly employed. While machine learning improves detection although faces challenges, adversarial attacks can fool ML models and manipulate ML-based malicious classifiers to escape exposure.

Deep Learning for Malware Detection: DL-based malwares detection schemes have attained respectable results when utilizing pre-trained large-scale models [36]. It can process enormous datasets with high accuracy, furthermore, utilizes neural networks to discover complex patterns, extract the features and classified. However, it demands considerable computational resources. In 2021 [37] introduced a DL-based for malwares classification framework, with transfer learning and hybrid architectures to achieve enhanced performance. Thus, the method realizes high accuracy through all datasets; 94.88% on Microsoft BIG 2015, 97.78% on Mailing, and 96.5% on Malevis [37]. D. Gibert et. al. [38] contrasting to usual machine learning approaches that depend on hand-engineered features, introduced HYDRA which integrates both deep learning and feature engineering using intermediate fusion of learned representations. HYDRA achieves 99.75% accuracy, and compared to signature-based methods, HYDRA is resistant to polymorphic and obfuscated malware. Since it detects malware based on multiple feature sources. In 2025, [39] applied multiple Convolutional Neural Networks (CNNs) to categorize malware with high accuracy.

The model was assessed on Drebin and AMD benchmark datasets, realizing 98.65% and 97.91% accuracy. That bypasses traditional feature engineering limitations. A. Alotaibi, [40] proposed MalResLSTM, a deep residual long short-term memory (LSTM) framework for Android malware revealing. The model was assessed on the Drebin dataset, realizing a 99.32% detection accuracy, bettering DL and traditional ML models. Ke He et. al. [41] studied DL-based network IDSs and their weakness against adversarial attacks. Whereas deep neural networks improve NIDS detection accuracy, they are vulnerable to adversarial perturbations, which can lead to misclassification. Network-based attacks need a special methodology due to variations in detection pipelines and feature spaces.

4. COMPARATIVE ANALYSIS OF AI-POWERED AND CONVENTIONAL APPROACHES

This section illustrates a comparative analysis of conventional malwares detection and AI-powered methods. It elaborates on every feature, providing deeper insights into the powers, restrictions, and implications of both tactics in the context of recent cybersecurity factors such as accuracy, adaptability, scalability, resource requirements, cost, and further. Signature-based or behaviour-based utilizing static or dynamic analysis are primary detection methods applied in conventional approaches. These methods identify known patterns professionally however struggle with novel malware. AI-powered detection, alternatively, engages machine learning, anomaly detection, and deep learning to recognize equally known and unknown malware risks. Via reducing dependence on predefined signatures, AI models develop security. Conventional detection methods grant moderate accuracy, particularly productive for known malware but lacking against developing patterns.

AI-powered methods via learning from vast datasets and realizing previously unseen models achieve higher accuracy. Nonetheless, performance of models depends on algorithm optimization, as well as quality and quantity of training data. Signature-based detection demonstrates high performance for acknowledged threats but continues vain against new malware. AI-driven detection, by comparison, bests at detecting both known and unknown threats. Furthermore, real-time detection effectiveness can be affected by computational overhead and model complexity. In terms of adaptability, traditional malware detection approaches rely on manual updates, as a result they are reactive rather than proactive. Their efficiency reduces when faced with advancing malware systems. AI-powered methods continuously learn and adapt to the dynamic nature of cyber threats, offering a proactive security mechanism. Traditional detection systems on average have low false positives since their reliance on clear signatures. AI-powered detection may produce a higher false positive ratio, based on training data and model optimization. Constant refinement of algorithms is crucial to balance specificity and sensitivity. Conventional methods consume minimal computational resources, making them ideal and efficient for smaller organizations or legacy systems. AI-powered methods required substantial computing power for training and inference, making them resource-intensive but offer superior detection capabilities and scalability.

Conventional methods are more applicable for detecting simple-coded attack patterns, while AI-driven approaches suited for analysing and recognizing modern and complex-coded threats. AI models are superior for defending against sophisticated cyberattacks due to their highly developed malware recognition. Signature-based detection is generally speedier in performance although slower in updating while new threats need manual updates to signature databases. AI-powered detection operates in real time, providing rapid classification and analysis. Therefore, during model learning phases the overhead training can introduce delays. Both approaches require maintenance, though conventional methods need continuous updates to signature databases to stay valuable. AI-powered detection requires periodic model retraining to feature new threat information, which can be resource-intensive but guarantees adaptability.

Traditional detection systems are less effective in large-scale networks due to restricted scalability. AI-powered techniques offer high scalability, adapting to growing cybersecurity requirements and capable of handling massive datasets. While AI-powered methods require a higher initial asset, they grant cost savings in the long cycle through automation and decreased maintenance. Conventional methods, though cheaper initial implementation, can become costly over time with manual efforts and frequent updates. AI-powered detection excels against zero-day threats, employing anomaly detection and predictive analytics to classify earlier unseen threats before they cause damage, while conventional methods perform poorly in this part due to their total dependence on known signatures.

Conventional methods are yet broadly used in restricted resources environments as enterprise solutions and legacy antivirus systems. AI-powered detection, for due to its improved capabilities, is broadly adopted in current cybersecurity solutions. AI-powered malware detection surpasses conventional methods in adaptability, scalability, and zero-day threat identification. While traditional approaches still relevant for basic malware protection, Figure 1, shows a radar chart comparing conventional and AI-powered malware detection approaches. Therefore, AI-powered methods present excel performance in accuracy, adaptability, scalability, and zero-day detection, as conventional methods demand fewer resources and have lower initial costs. In conclusion, organizations should integrate AI-driven mechanisms to strengthen their cybersecurity shield and guarantee robust, future-proof security solutions.

5. HYBRID APPROACHES AND FUTURE TRENDS

Despite improvements, malware detection remains a challenging subject due to the continuous evolution of malware schemes. The main challenges include, *Zero-Day Threats*: The previously discovering unknown malware remains a substantial challenge [42]. *Scalability*: The exponential expansion of malware samples demands scalable detection systems [43]. *Evasion Techniques*: Malware authors consistently use approaches such as code obfuscation and polymorphism to escape detection [44-45]. Combining traditional and AI-based methods can alleviate their corresponding weaknesses. Such as hybrid develops use signature-based detection for realized threats while engaging ML/DL for adaptive analysis. Additionally, data mining methods can extract malware features, enabling the development of new datasets and detection models. There are diverse models such as graph and n-gram models to create malware datasets and features. However, Malware detection is an endless fight between defenders and attackers. Forthcoming research should give attention to optimizing AI models for computational cost reduction, improve efficiency, and enhance explainability for advance trust and adoption in real-world scenarios. Scalability should also be enhanced to support large-scale cybersecurity applications.

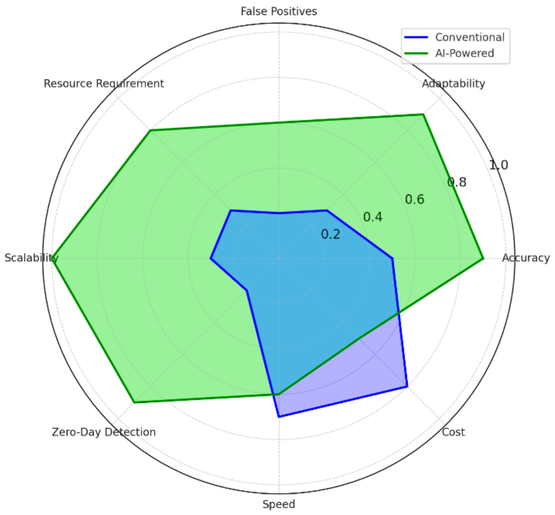

Figure 1. Conventional vs AI-powered malware detection approaches.

6. CONCLUSIONS

Malware analysis and detection are crucial components of cybersecurity. While traditional methods like signature-based detection remain effective, the growing complexity of malware demands advanced methods such as behaviour-based analysis with machine learning. A combination of tactics and tools allows practitioners and researchers to stay ahead of progressing threats and protect digital systems effectively. For example, selecting the right malware detection method is critical for saving your organization versus evolving malware threats. With a varied range of available tools, it’s important to focus on solutions that align with your given requirements and provide robust protection. In this article, a extensive study of conventional and AI- powered malware detection approaches has been provided. Consequently, the paper presents a comparison of existing models, their strengths and limitations in terms of adaptability, accuracy, resource requirements, cost, scalability and more. Finally, the paper also highlights future research directions. Thus, the focus is transforming to optimizing AI models to reduce computational costs, improve efficiency, and enhance explainability for real-world scenarios.

REFERENCES

[1] Gu, Y., 2023. A survey of traditional and machine learning-based malware detection techniques. IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA).

[2] Saeed, M. M., et al., 2025. A lightweight protocol to enhance privacy in wireless-enabled 5G networks for industrial internet of things (IIoT) communications. Security & Privacy 8(5), e70083.

[3] Hassan, M. B., et al., 2022. Green machine learning for green cloud energy efficiency. 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), pp. 288–294.

[4] Maniriho, P., Mahmood, A. N., Chowdhury, M. J. M., 2024. A systematic literature review on Windows malware detection: techniques, research issues, and future directions. J. Syst. Softw. 209, 111921.

[5] Aboaoja, A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., 2022. Malware detection issues, challenges, and future directions: a survey. Appl. Sci. 12(17), 8482.

[6] Yunmar, R. A., et al., 2024. Hybrid Android malware detection: a review of heuristic-based approach. IEEE Access 12, 41255–41286.

[7] Saeed, M. M., et al., 2023. Machine learning techniques for detecting DDOS attacks. 3rd Int. Conf. on Emerging Smart Technologies and Applications (eSmarTA), Taiz, Yemen, pp. 1–6.

[8] M., A., Saldanha, A., 2020. Malware analysis and detection engineering. Springer Nature.

[9] Mata-Torres, J. A., et al., 2023. Evaluation of machine learning techniques for malware detection. Intell. Syst. Ref. Libr. 226, 121–140.

[10] Aslan, O., Samet, R., 2020. A comprehensive review on malware detection approaches. IEEE Access 8, 6249–6271.

[11] Mokhtar, R., Saeed, R. A., 2011. Conservation of mobile data and usability constraints, in: Junaid, Z., Athar, M. (Eds.), Cyber Security Standards, Practices, and Industrial Applications: Systems and Methodologies, Ch. 03, IGI Global, USA, pp. 40–55.

[12] Kamble, M. T., Sridevi, 2022. Feature extraction and analysis of portable executable malicious file, in: 2nd Int. Conf. on Computer Science, Engineering and Applications (ICCSEA).

[13] Gadal, S., Mokhtar, R., Abdelhaq, M., Alsaqour, R., Ali, E. S., Saeed, R., 2022. Machine learning-based anomaly detection using K-mean array and sequential minimal optimization. Electronics 11, 2158.

[14] Ma, Y., Han, L., Ying, H., Yang, S., Zhao, W., Shi, Z., 2019. SVM-based instruction set identification for grid device firmware, in: Proc. IEEE 8th Joint Int. Information Technology and Artificial Intelligence Conf. (ITAIC), pp. 214–218.

[15] Nar, M., Kakisim, A. G., Yavuz, M. N., Sogukpinar, I., 2019. Analysis and comparison of disassemblers for opcode based malware analysis, in: UBMK 2019 – 4th Int. Conf. on Computer Science and Engineering, pp. 17–22.

[16] Saeed, M. M., et al., 2023. Attacks detection in 6G wireless networks using machine learning, in: 9th Int. Conf. on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, pp. 6–11.

[17] Votipka, D., Stevens, R., Redmiles, E., Hu, J., Mazurek, M., 2018. Hackers vs. testers: a comparison of software vulnerability discovery processes, in: Proc. IEEE Symp. on Security and Privacy, pp. 374–391.

[18] Ahmed, M. N., 2023. Analyzing OneNote malware through static and dynamic analysis: detection and mitigation measures, in: Int. Conf. on IT and Industrial Technologies (ICIT).

[19] G., P., Goyal, A., 2017. Comparative study of two most popular packet sniffing tools - Tcpdump and Wireshark, in: 9th Int. Conf. on Computational Intelligence and Communication Networks, pp. 77–81.

[20] Nguyen, H. N., et al., 2022. MalView: interactive visual analytics for comprehending malware behavior. IEEE Access 10, 99909–99930.

[21] Singh, J., Singh, J., 2021. A survey on machine learning-based malware detection in executable files. J. Syst. Archit. 112, 101861.

[22] Li, J., Li, Q., Zhou, S., Yao, Y., Ou, J., 2017. A review on signature-based detection for network threats, in: 9th IEEE Int. Conf. on Communication Software and Networks (ICCSN), pp. 1117–1121.

[23] Almutairi, A. H., Abdelmajeed, N. T., 2017. Innovative signature based intrusion detection system, in: Int. Conf. on the Frontiers and Advances in Data Science, pp. 114–119.

[24] Al-Asli, M., Ghaleb, T. A., 2019. Review of signature-based techniques in antivirus products, in: Int. Conf. on Computer and Information Sciences (ICCIS), pp. 1–6.

[25] Abbas, T., Srikanthan, M. F., 2017. Low-complexity signature-based malware detection for IoT devices, in: Applications and Techniques in Information Security, pp. 181–189.

[26] Bahador, M. B., Abadi, M., Tajoddin, A., 2019. HLMD: a signature-based approach to hardware-level behavioral malware detection and classification. Springer US 75(8).

[27] Kwon, H. Y., Kim, T., Lee, M. K., 2022. Advanced intrusion detection combining signature-based and behavior-based detection methods. Electronics 11(6), 1–19.

[28] Galal, M. A., Mahdy, H. S., Atiea, Y. B., 2016. Behavior-based features model for malware detection. J. Comput. Virol. Hacking Tech. 12, 59–67.

[29] Hu, S., Xiao, Z., Rao, Q., Liao, R., 2018. An anomaly detection model of user behavior based on similarity clustering, in: Proc. IEEE 4th Information Technology and Mechatronics Engineering Conf. (ITOEC), pp. 835–838.

[30] Bharathy, A. M. V., Umapathi, N., Prabaharan, S., 2019. An elaborate comprehensive survey on recent developments in behaviour based intrusion detection systems, in: 2nd Int. Conf. on Computational Intelligence in Data Science (ICCIDS), pp. 1–5.

[31] Gaber, M. G., Ahmed, M., Janicke, H., 2024. Malware detection with artificial intelligence: a systematic literature review. ACM Comput. Surv. 56(6).

[32] Hosna, A., Tabassum, N., Supriya, R., et al., 2024. Enhancing health-care security: the role of blockchain and consensus mechanisms. AIH 0(0), 2580.

[33] Martins, N., Cruz, J. M., Cruz, T., Henriques Abreu, P., 2020. Adversarial machine learning applied to intrusion and malware scenarios: a systematic review. IEEE Access 8, 35403–35419.

[34] Hasan, M. K., et al., 2022. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Commun. 16, 421–432.

[35] Ali, E. S., et al., 2021. Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. J. Secur. Commun. Netw., Article ID 8868355.

[36] Miao, C., Kou, L., Zhang, J., Dong, G., 2024. A lightweight malware detection model based on knowledge distillation. Mathematics 12(24), 1–13.

[37] Aslan, O., Yilmaz, A. A., 2021. A new malware classification framework based on deep learning algorithms. IEEE Access 9, 87936–87951.

[38] Zeinab, A. E., Saeed, R. A., Mukherjee, A., 2019. Challenges and opportunities in vehicular cloud computing, in: Cloud Security: Concepts, Methodologies, Tools, and Applications, IGI Global, Hershey, PA, pp. 2168–2185.

[39] Saeed, M. M., et al., 2023. Anomaly detection in 6G networks using machine learning methods. Electronics 12, 3300.

[40] Alotaibi, A., 2019. Identifying malicious software using deep residual long-short term memory. IEEE Access 7, 163128–163137.

[41] Ali, E. S., Saeed, R. A., 2014. A survey of big data cloud computing security. Int. J. Comput. Sci. Softw. Eng. (IJCSSE) 3(1), 78–85.

[42] Aboaoja, F. A., et al., 2022. Malware detection issues, challenges, and future directions: a survey. Appl. Sci. 12(17), 8482.

[43] Elmubark, M. A., et al., 2015. Fast and secure generating and exchanging a symmetric keys with different key size in TVWS, in: Int. Conf. on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), Khartoum, Sudan, pp. 114–117.

[44] Amer, S. E. E., Zelinka, I., 2021. A multi-perspective malware detection approach through behavioral fusion of API call sequence. Comput. Secur. 110, 102449.

[45] Saeed, M. M., Ali, E. S., Saeed, R. A., 2023. Data-driven techniques and security issues in wireless networks, in: Data-Driven Intelligence in Wireless Networks: Concepts, Solutions, and Applications, Ch. 7, CRC Press.