THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 1.1 (2025)
https://doi.org/10.62019/abbdm.v5i3.351

A Systematic Literature Review on AI-Based Methods for Malware Detection

Anna Tariq, Arshad Mehmood

Chronicle

Article history
Received: May 2, 2025
Received in the revised format: June 20, 2025
Accepted: July 1, 2025
Available online: July 11, 2025

Anna Tariq, & Arshad Mehmood are currently affiliated with the Department of Information Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan, Pakistan.
Email: annaazam1999@gmail.com
Email: arshad.mehmood1@riphah.edu.pk

Corresponding Author* Anna Tariq

Abstract

Recent breakthroughs in artificial intelligence have improved malware detection, allowing systems to discover new threats by recognizing unexpected patterns that go beyond established signatures. AI-driven detection is critical in cybersecurity, and it covers malware detection, intrusion detection, and phishing prevention. This review investigates AI-based malware detection studies from (2015-2024) with a focus on machine learning and deep learning techniques. It emphasizes improvements in dealing with complex malware, including polymorphic and file less variants, while also highlighting obstacles like as high computing costs and data issues. The study emphasizes AI's potential for enhanced detection and encourages future research on real-time, resource-efficient, and interpretable models.

Keywords: Malware Analysis, Transfer Learning, Static Analysis, Dynamic Analysis, Machine learning, Deep learning.

© 2025 The Asian Academy of Business and social science research Ltd Pakistan.

INTRODUCTION

Network intrusion detection seeks to detect harmful traffic such as DoS, DDoS, botnets, malware, crypto jacking, and data theft (Geenens, 2019). Phishing detection focusses on preventing scams that steal personal information or redirect to hazardous websites. However, this study focusses on malware identification, which includes recognizing viruses, Trojans, ransomware, crypto miners, worms, bots, and other malware (Dargahi et al., 2019). AI-based malware detection is critical because malware is growing with evasion strategies, such as anti-analysis and packaging methods, that frustrate static and dynamic analysis tools like disassemblers, debuggers, and sandboxes (Suraneni, 2022) (Dukarm, 2020). As signature-based detection becomes less effective, anomaly detection technologies that rely on pattern recognition provide a more robust alternative for identifying malware.

AI based Techniques for Malware Detection

AI-based malware detection has improved significantly thanks to machine learning and deep learning approaches, which improve accuracy in detecting new and emerging threats. Neural networks, particularly deep learning models such as RNNs and CNNs, are excellent at recognizing complicated patterns in system and network behavior. Decision trees offer transparent classification into benign or harmful categories, but SVMs successfully identify normal from malicious activity, especially in high-dimensional data. Collectively, these strategies improve malware detection capabilities. Random Forests use several decision trees to improve malware detection accuracy and prevent overfitting, making them ideal for datasets with a large number of features. Ensemble approaches, such as Boosting and Bagging, integrate numerous models (e.g., decision trees, SVMs, and neural networks) to improve detection rates and reduce false positives. Overall, AI techniques including as neural

networks, decision trees, SVMs, and ensemble algorithms are extremely effective at accurately and consistently classifying malware and detecting developing, sophisticated threats.

Figure 1.
Taxonmy of the Malware Detection using AI

Hybrid AI Approaches for Malware Detection

Hybrid AI models improve malware detection by combining static and dynamic analytic techniques, which overcome the limits of standard signature-based methods. These integrated approaches increase accuracy, particularly against polymorphic and obfuscated malware, by utilizing AI technologies such as decision trees, SVMs, and neural networks. Despite data constraints, hybrid systems provide more effective, adaptive, and robust solutions for detecting emerging and complex threats, outperforming traditional approaches. Hybrid approaches increase malware detection by combining static and dynamic techniques in a single system, which outperforms any method alone. Combining machine learning with deep learning, such as decision trees or random forests (Raff et al., 2020), classifies malware based on extracted features, whereas CNNs and RNNs analyses raw byte or execution sequences. In addition, these hybrid techniques improve interpretability and efficiency when dealing with vast amounts of unstructured data (Shafiq et al., 2022).

Transfer Learning in Malware Detection

Transfer learning improves malware detection by allowing models to shift from one domain to another with minimum retraining, saving both time and resources (El-Shafai et al., 2021). For example, a model trained on Windows malware can be simply adapted to Android. It also allows for cross-domain detection, such as using Trojan-trained models to detect ransomware (Deldar et al., 2023). This method enhances performance, particularly for zero-day malware, by allowing for rapid adaptability and improved generalization, making it more practical and efficient (Thanh et al., 2019, December).

Challenges in Malware Detection

AI-generated anti-malware programs have advanced, but there are still a number of issues. Training data quality is crucial since malware tactics like encryption and obfuscation quickly stale datasets, which affect AI performance (Minhaj, 2023). Malware can evade detection by using adversarial instances, which are little disruptions intended to trick models (Shamshirband et al., 2020). Furthermore, real-time detection is limited by the computational expense of evaluating big data volumes, particularly on devices with limited resources like mobile phones or the Internet of Things (Ye et al., 2017). It is still challenging to guarantee that models are accurate and effective in a variety of dynamic malware scenarios, especially as malware grows increasingly complex to avoid detection (Thakur et al., 2024). While robust systems remain a difficulty, hybrid AI techniques and transfer learning enhance the detection of emerging risks (Jimmy, 2021). Future AI-based cybersecurity solutions must overcome adversarial attacks, problems with data quality, and processing needs (Luo et al., 2021).

SIGNIFICANCE/CONTRIBUTION

This study offers a thorough analysis of contemporary malware detection techniques, highlighting the ways in which artificial intelligence (AI), particularly machine learning and deep learning, improves accuracy, scalability, and responsiveness to new threats.
Examining existing methods to determine the best AI strategies.
Assessing the effectiveness of these AI techniques in malware detection and mitigation.
Grouping AI techniques according to their appropriateness and efficacy.
Outlining the advantages and disadvantages of different AI strategies.
Providing analysis and suggestions for improving malware detection using AI in the future.

LITERATURE REVIEW

Since traditional methods—aside from signature-based ones—struggle with more complex malware, AI-based malware detection has gained traction (Alsoufi et al., 2021). By examining patterns in system data, CNNs and RNNs make it possible to identify novel and zero-day threats. The efficacy of these AI methods in malware detection is evaluated in a systematic review (Fernandes et al., 2019). Since traditional methods—aside from signature-based ones—struggle with more complex malware, AI-based malware detection has gained traction (Alsoufi et al., 2021). By examining patterns in system data, CNNs and RNNs make it possible to identify novel and zero-day threats. The efficacy of these AI methods in malware detection is evaluated in a systematic review (Fernandes et al., 2019).

AI based methods for Malware Detection

AI techniques are becoming more and more important for identifying anomalous system activity that could be a sign of malware (De Spiegeleire et al., 2017). AI—particularly deep learning (DL) and machine learning (ML)—improves the identification of new malware, in contrast to signature-based techniques, which are sluggish against developing threats (Pirscoveanu et al., 2015, June). Both supervised and unsupervised machine learning approaches are widely used: supervised models employ labeled data, whilst unsupervised models detect behavioral anomalies; reinforcement learning is also being investigated for adaptive detection (Akhtar et al.,

2022). Both CNNs and RNNs are powerful deep learning tools; auto encoders learn and spot system behavior anomalies, CNNs analyze massive amounts of data, and RNNs record temporal patterns (Ozkan-Okay et al., 2024). Combining AI methods, such as static and dynamic analysis, increases the accuracy of detection, particularly when dealing with sophisticated malware, such as stealth or polymorphic variants (Caviglione et al., 2020), (Farooq, 2023).

Types of Malware

Finding different kinds of malware, such as viruses, worms, Trojan horses, ransomware, spyware, adware, rootkits, botnets, and zero-day threats, is the main objective of AI-based malware detection (Capuano et al., 2022). By examining patterns of system activity, AI models can learn the distinct behaviors displayed by these virus varieties. For example, botnets can be identified by their distinctive network traffic patterns resulting from external server contact, whereas ransomware frequently causes quick file encryption (Capuano et al., 2022). Trojan horses pose as trustworthy programs, therefore it's important to keep an eye on their activity to spot them. By adapting to identify both known and novel malware behaviors, deep learning models such as CNNs and RNNs can enhance the detection of new threats (Gaber et al., 2024).

Table 1. Literature Review Summary

Paper Name	Year	Publisher	Contribution	Limitation	Summary
Malware _Detection with Artificial Intelligence: A Systematic Literature Review (Gibert et al., 2020)	2024	ACM	Examines significant advancements in AI for malware identification	Studies asserting that DL is better than ML and vice versa have contradictory findings. - Poor quality datasets make it difficult to extract genuine features from complex viruses.	The study thoroughly examines developments in AI for malware detection, stressing the significance of feature quality and dataset appropriateness while tackling the difficulties presented by complex malware and analytic methods.
A Survey on Machine Learning_ Techniques for Cyber Security in the Last Decade (Shaukat et al., 2020)	2020	IEEE	The research investigates how the Internet alongside mobile app adoption spreads rapidly along with enhanced exposure to cyber threats because of automated and persistent attacks. Traditional security	Although the paper lacks precise boundary conditions it functions as an survey which potentially fails to tackle individual techniques while missing new experimental findings.	This paper examines how cyberspace continues to develop while explaining why advanced protection methods are crucial for detecting modern complex cyber intrusions. Previous security systems demonstrate their limited

			approaches remain insufficient because cyber attackers continuously create new advanced security evasion tactics.		effectiveness when faced with hackers who use deceptive cyberattack strategies.
Dynamic Malware Analysis in the Modern Era—A State of the Art Survey (Or-Meir et al., 2019)	2019	ACM	Extensive analysis of recent malware dynamic procedures which explains fundamental functionalities of each method and its defense capabilities against malware evasion mechanisms. The analysis includes an evaluation of various landmark investigations which demonstrate the application of machine-learning strategies for improving sophisticated security operations in dynamic malware analysis detection alongside categorization dynamics.	Modern dynamic analysis methods do not provide perfect results since no single solution exists to examine full malware behaviors	Examines escalating malware assaults since recent years while emphasizing protection requirements through unambiguous detection. The paper demonstrates that static analysis techniques have fundamental limitations due to malware authors' use of evasion mechanisms while recommending dynamic analysis as a more comprehensive detection method. The study provides detailed information about different dynamic analysis methods together with their practical applications as well as how machine learning enhances detection systems.
A Comprehensive Review on Malware	2019	IEEE	Dramatic rise of malicious software across networks	Fails to detail particular implementation constraints because it does not establish new	A detailed exploration of diverse malware

Detection Approaches (Ucci et al., 2019)			alongside malicious strategies used by malware to conceal itself. The detection of malware requires advanced methods to ensure computer systems remain secure both on the Internet and within other networks.	experimental research findings or create innovative detection solutions.	detection methods while evaluating their ability to identify and stop security threats. Also examines obstacles created by modern obfuscation approaches while underlining the significance of creating dependable protection approaches to secure networks from rising malware threats.
Malware Detection with Artificial Intelligence: A Systematic Literature Review (Mimura et al., 2022)	2022	ACM	Provides a comprehensive review of AI-based malware detection methods, particularly deep learning. Highlights trends and challenges.	The study lacks empirical testing and practical application examples.	The paper gives a thorough overview of AI's role in detecting malware, emphasizing deep learning techniques. It discusses the evolution of AI-based methods, the importance of data quality, and highlights challenges such as adversarial attacks and detection of evolving malware.
Applying NLP Techniques to Malware Detection in a Practical Environment (Mehta et al., 2024)	2024	Springer	Provides a novel application of NLP techniques to improve malware detection accuracy in real-world settings.	Practical implementation may face issues related to computational cost and scalability.	This study demonstrates the potential of NLP techniques in detecting malware in practical scenarios, offering insights into the challenges of deploying machine learning models in real-time environments. The evaluation of efficiency and accuracy highlights both

					strengths and areas for improvement, especially concerning scalability.
A Natural Language Processing Approach to Malware Classification [(Karbab et al., 2021)	2021	Springer	Introduces a new approach for malware classification using NLP and HMMs. Demonstrates effectiveness of opcode sequences in classification.	Limited to a specific set of data; the approach may not generalize well to all types of malware.	The paper explores an innovative NLP approach, applying Hidden Markov Models to opcode sequences for malware classification. This method shows strong performance in detecting known malware, though the system's adaptability to newly emerging or unknown malware types is still a challenge.
Resilient and Adaptive Framework for Large Scale Android Malware Fingerprinting using Deep Learning and NLP Techniques (Maniriho et al., 2022)	2022	Springer	Proposes an adaptive framework for large-scale Android malware detection, leveraging both deep learning and NLP for greater accuracy.	The complexity of the system might make it difficult to scale effectively in resource-constrained environments.	The study proposes an innovative framework that combines deep learning with NLP techniques for efficient Android malware fingerprinting. It addresses challenges in scalability and resilience, providing a robust approach for large datasets, but struggles with real-time application in low-resource environments.
MalDetConv: Automated Behaviour-based Malware Detection Framework Based on Natural Language Processing and	2024	MDPI	Combines behavioral analysis with deep learning and NLP for detecting sophisticated malware,	The framework's effectiveness may be impacted by false positives and its adaptability to new malware behaviors.	MalDetConv integrates behavioral analysis, NLP, and deep learning for malware detection. It stands out in its

Deep Learning Techniques (Yunmar et al., 2024)		including zero-day attacks.		ability to detect zero-day malware, but challenges remain in handling false positives and ensuring the framework's adaptability to dynamic malware behaviors.
Hybrid Android Malware Detection: A Review of Heuristic-Based Approaches (Taher et al., 2023)	2023 IEEE	Summarizes advancements in heuristic-based methods, offering a comprehensive look at hybrid approaches for malware detection.	Heuristic methods can struggle with evolving or sophisticated malware.	The paper provides an extensive review of heuristic-based approaches in Android malware detection, discussing their effectiveness, especially in hybrid models. The paper notes the challenges of detecting advanced or evolving malware and the need for hybrid systems that combine multiple detection techniques.
DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection (Demetrio et al., 2021)	2021 MDPI	Introduces a hybrid model combining static and dynamic analysis, improving malware detection accuracy on Android devices.	Performance could degrade on highly obfuscated malware or malware with low activity.	DroidDetectMW presents a hybrid approach, integrating static and dynamic analysis methods to detect Android malware. By combining machine learning and deep learning techniques, it improves detection accuracy, though challenges remain in dealing with obfuscated malware or

					those exhibiting low activity.
Adversarial Malware Detection with Deep Learning: A Survey (Bruna Moralejo, 2023)	2023	Springer	Highlights the use of deep learning for adversarial malware detection and methods to improve resilience against attacks.	The techniques discussed may not fully address the evolving nature of adversarial threats.	The survey explores deep learning applications in adversarial malware detection, discussing how these methods can be fortified against adversarial attacks. Despite promising solutions, the paper points out the need for continuous adaptation due to the evolving nature of adversarial threats.
Machine Learning for Malware Detection and Classification (Ali et al., 2022)	2022	IEEE	Provides a comprehensive overview of machine learning applications in malware detection, covering various algorithms and evaluation metrics.	The reliance on traditional feature extraction methods can limit the detection of more sophisticated malware.	The paper reviews how machine learning methods are applied to malware detection, focusing on feature extraction and classification techniques. While effective for standard malware, the methods discussed are less effective against more sophisticated or previously unseen threats.
Deep Learning Techniques for Malware Detection: A Review of Approaches and Applications (Chakkaravarthy et al., 2019)	2019	IEEE	Offers a detailed review of deep learning architectures for malware detection and their success in identifying diverse threats.	The high computational costs of deep learning models may make them impractical for real-time malware detection.	The paper presents an in-depth review of deep learning architectures like CNNs and RNNs for malware detection. These methods show significant promise in identifying a wide range of malware,

	though they face challenges in real-time application due to high computational demands.

LIMITATION

Current research lacks comprehensive systematic reviews on hybrid and transfer learning approaches in malware detection. Combining these strategies shows great potential for improving detection performance and adapting to evolving threats. Focusing on integrating hybrid and transfer learning can significantly enhance malware detection capabilities.

METHODOLOGY

Review Method

This study follows best practices for systematic literature reviews in software engineering, with a focus on AI-based malware detection. It compares methodologies, stresses hybrid solutions, and investigates methods for better detecting advanced and stealthy malware.

The Need for Systematic Review

With the growing interest in AI for malware detection, more research is being published, but a thorough evaluation of anomaly detection methods is absent. Traditional signature-based approaches are no longer effective against emerging, elusive malware, such as zero-day threats. This SLR seeks to close that gap by reviewing research on AI-based anomaly detection, including as static and dynamic analysis, feature selection, and integrated techniques.

The Review Protocol

The review methodology is crucial for directing the selection of studies, guaranteeing objectivity, and preventing bias. It explains how to choose studies, create questions, gather data, and combine findings.

It is the case that this SLR has been designed to address the following critical research questions:

- What are the most effective methods in AI for identifying malware?
- How effective are existing artificial intelligence approaches in detecting and mitigating malware?

Data Extraction and Study Selection:

The IEEE, Web of Science, Scopus, Science Direct, and MDPI databases were searched for this review, with an emphasis on peer-reviewed DOI, full-text English publications published between 2015 and 2024, and articles that used AI to detect malware. Static/dynamic analysis, merging AI approaches, and problems like high false positives, computing costs, and dataset restrictions were used to categorize the studies.

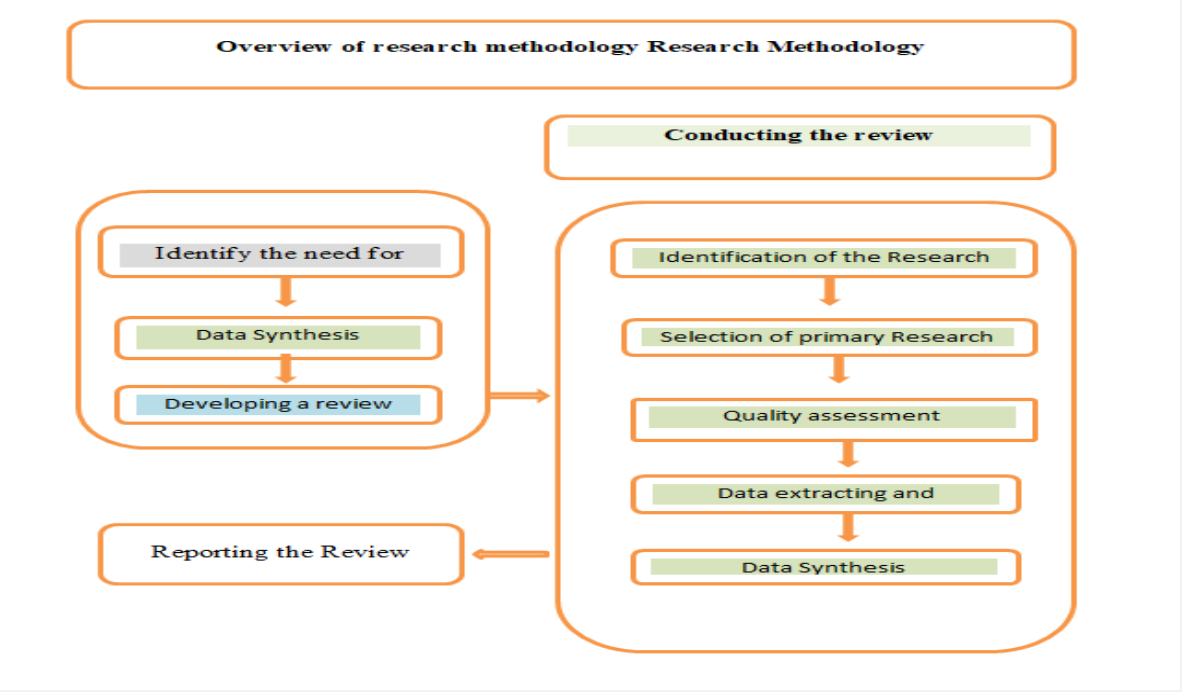

Figure 2.
Research Methodology

Data Synthesis:

To find fresh themes, strategies, and avenues for future study in AI-based malware detection, these studies will be compiled and examined. The efficacy of multi-strategy methods, combination methodologies, and transfer learning in overcoming the drawbacks of conventional anti-malware systems will be highlighted in the synthesis.

Search Strategy

This SLR, which employs large databases, focuses on AI techniques for malware detection from 2015 to 2024, namely ML and DL (such as CNNs and RNNs). It covers research on anomaly detection, feature extraction, transfer learning, and static/dynamic analysis. The review demonstrates how integrating AI with conventional methods enhances detection and lowers false positives for sophisticated, covert malware.

Primary Records Selection

Books, reports, and secondary sources published between 2015 and 2024 were first sifted by abstracts and titles in order to concentrate on original, peer-reviewed research. High-quality ML or DL methods, such as feature selection and static/dynamic analysis, must be used in the chosen studies for anomaly-based malware detection. The selection process was carried out by two independent assessors, with a third settling disputes to guarantee that only the most trustworthy and pertinent documents were included.

Secondary Records Selection

The chosen papers were subjected to a secondary filter based on eligibility standards developed from the research topics. The analysis only includes pertinent research on AI-based anomaly detection in malware over the previous five years, with an emphasis on feature selection, malware complexity, hybrid approaches, and transfer learning.

CRITERIA FOR INCLUSION

Type of Publication

Technical reports, conference papers, and peer-reviewed journal articles released from 2014 to 2024. Pay particular attention to research on malware detection, AI, deep learning, and machine learning approaches in cybersecurity, especially studies that combine static and dynamic analysis methodologies. Pay close attention to articles that examine transfer learning, particularly those that deal with heuristically constructed malware and zero-day malware.

Range of Publications (Published in the years 2014–2024)

- **Language** Only research that has been published in English or another selected language.
- **Applicability to the Research Question** Talk specifically about malware detection, AI cybersecurity techniques, transfer learning, zero-day malware, or static/dynamic analysis techniques that are in line with the state of the art.
- **Research Design** Experiments, case studies, qualitative analysis, and empirical research with a thorough methodology.
- **People/Domain** Centered on cybersecurity domains, particularly IoT security, healthcare systems, malware detection, or adjacent fields if indicated
- **Availability of Data** Research having easily available data, repeatable outcomes, or a thorough approach.
- **Study Quality** Satisfies established quality standards, such as thorough analysis, methodological rigor, and clarity.

Exclusion Criteria

- **Sources that are not peer-reviewed** Blogs, editorials, white papers, opinion articles, and other sources that aren't peer-reviewed should be excluded.
- **Multiple Publications** Studies that have been published more than once under various names will only be included in the most recent or thorough edition.
- **Unrelated Subjects** Research that has nothing to do with zero-day malware, transfer learning, AI in cybersecurity, malware detection, or static/dynamic analysis methods.
- **Not Enough Details** Lack of methodological specifics, ambiguous findings, or missing data; studies with inadequately stated goals or data abstraction techniques
- **Timeframe Outside of Scope** Publications that were not completely accessible, published prior to January 1, 2005, or outside of the 2014–2024 timeframe (if applicable).
- **Languages Other Than English** Unless multilingual sources are cited, studies published in languages other than English are excluded.
- **Only theoretical (if applicable)** Studies that are only theoretical and lack empirical support or implementation details should be excluded.
- **Poor Evaluation Results** Research that does not satisfy quality standards according to predetermined evaluation criteria (e.g., clarity, methodology robustness).

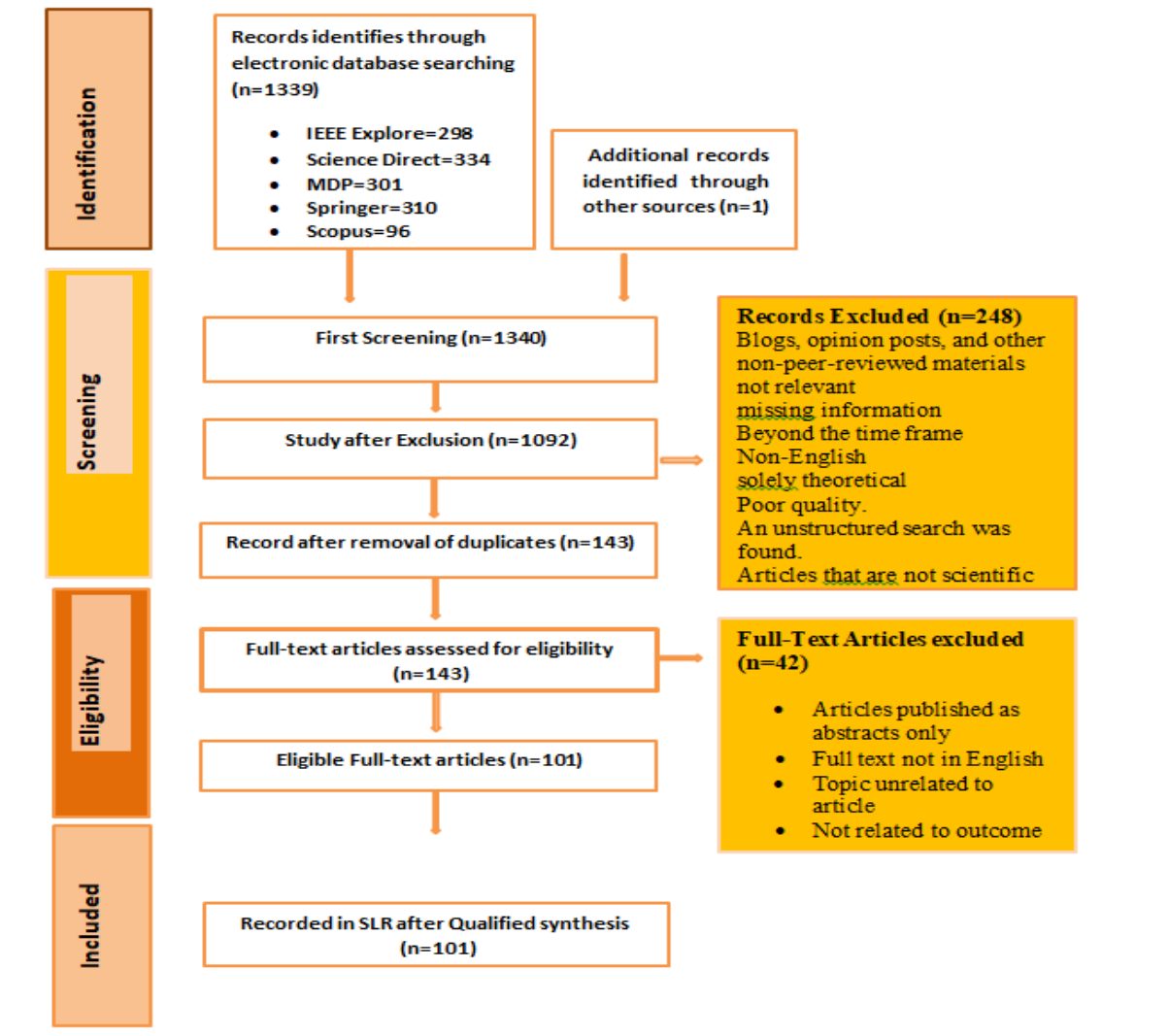

Figure 3.
Flowchart Showing how literature collected and process

Quality Assessment (QA) of the Eligible Included Records

These inquiries serve as the foundation for evaluating the quality of the study:
1. Are suitable AI-based malware detection papers explicitly defined by the criteria?
2. Is every pertinent piece of research thoroughly covered in the review?
3. Have the studies' validity and quality been adequately assessed?
4. Are the conclusions, data, and methods sufficiently explained and pertinent?

Data Extraction and Synthesis of the Systematic Literature Review

To systematically collect study details, such as ID, author, date, methods (e.g., CNN, SVM), and performance measures (accuracy, precision, recall, F1 score, FPR, FNR), the data extraction form was created using EndNote and Excel. To maintain objectivity, two researchers separately retrieved data, concentrating on transfer learning trends and static/dynamic analysis for better virus identification.

RESULTS AND DISCUSSION

Table 2 presents eight key insights from malware detection research between 2015 and 2024. It shows that ML models like Decision Trees, SVM, and Neural Networks

achieve high accuracy (70 papers). Dataset diversity is a challenge, affecting model generalization (50 papers). Dynamic analysis provides better detection but is slower, while static analysis is faster but easier to bypass (60 papers). Feature selection, such as API calls, enhances models (55 papers). Real-time detection remains difficult (65 papers). Deep learning methods like CNNs and RNNs have grown since 2018 (55 papers). There's emphasis on interpretable AI that adapts to different datasets (40 papers). Persistent issues include malware evolution, class imbalance, and adversarial attacks (45 papers). Despite progress, significant challenges remain.

Table 2.
key findings from the selected literature (2015-2024)

S .No	Finding/Insight	Significance/Description	Number of papers(2015-2024)
1	High ML Technique Effectiveness	High malware detection accuracy is attained by ML models such as Decision Trees, SVM, and Neural Networks.	70
2	Challenges of Dataset Diversity	Model generalization is impacted by a lack of large, varied datasets; well-known datasets include CICIDS, Kaggle, and others.	50
3	Analysis: Static versus Dynamic	Dynamic analysis provides greater detection but is slower than static analysis, which is quick but easily obfuscated.	60
4	The Value of Feature Selection	Models are enhanced by appropriate feature extraction (API calls, byte sequences).	55
5	Real-time detection is necessary.	The difficulty of attaining high-speed, low-latency detection.	65
6	The Deep Learning Trend	Since 2018, the use of CNNs, RNNs, and auto encoders has grown.	55
7	Transferable and comprehensible AI	Pay attention to interpretability and models that adjust to different datasets.	40
8	New Challenges	Class imbalance, virus evolution, and adversarial attacks continue to be major problems.	45

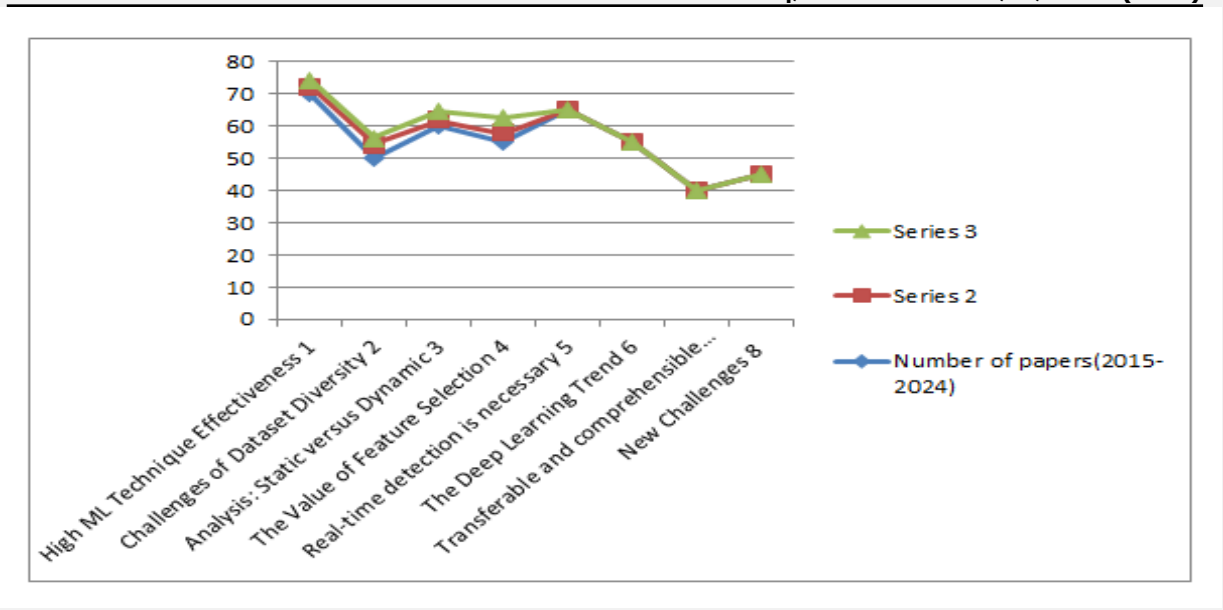

Figure4.
The key findings from the selected literature Graph

What are the most effective methods in AI for identifying malware?

The development of AI-based malware detection is examined in this systematic review (2015–2024), which focuses on a number of techniques such as transfer learning, deep learning, and static/dynamic analysis. It addresses advantages and disadvantages, forecasts future trends, and emphasizes the synergy of several AI techniques for increased detection rates with fewer false positives. The research highlights the growing significance of transfer learning and hybrid models in enhancing cybersecurity and thwarting sophisticated threats. In order to avoid detection, modern malware is always evolving table 3 highlight this. Cybercriminals are using increasingly complex strategies including hiding, disguising code, appearing innocuous, or activating only under particular circumstances. More efficient, creative solutions are required to address these issues, as traditional signature-based detection techniques are becoming antiquated (Chakkaravarthy et al., 2019).

Table 3.
Types of Malware Sophistication

Malware Type	Description
Polymorphic Malware	Changes its code on every execution to avoid detection.
Metamorphic Malware	Completely rewrites its code to create a new version every time.
Rootkits	Hides its presence from detection tools and alters system files.
File less Malware	Operates in memory and does not write files to disk, evading detection.

Static & Dynamic Analysis

Static analysis examines code without executing it, while dynamic analysis studies behavior when the file is run in a safe environment (Hassen et al., 2017, November).

Static Analysis It is the initial step in malware detection, examining files for malicious code, strings, or instructions without execution. It is fast and safe but can miss obfuscated or encrypted malware [60]. Sub-models include signature-based detection (identifying known malware signatures), disassemblers/decompilers (like IDA Pro and Ghidra) for analyzing code structure, and control flow graphs (CFG) to examine program execution flow for abnormal behavior.

Dynamic Analysis It involves executing malware in a controlled environment (sandbox) to observe its behavior, such as network activity, file changes, and system modifications. It is especially useful for detecting file less or behavior-dependent malware. Sub-models include behavioral analysis (tracking actions during execution), memory analysis (examining in-memory malware), and system call analysis (monitoring system calls for suspicious activity).

Table 4.
Static and Dynamic Analysis

Analysis Type	Techniques/Tools	Description
Static Analysis	Signature-based Detection, Disassemblers, Control Flow Graphs	Analyzes the file's code or structure without execution.
Dynamic Analysis	Behavioral Analysis, Memory Analysis, System Call Analysis	Observes the behavior of a file during execution.

Malware Datasets In order to enable ML and DL models distinguish between safe and dangerous files or actions, datasets with examples of both malicious and benign software are essential for training these models in malware detection.

CICIDS 2017. For the purpose of training malware and anomaly detection algorithms, it offers CIC's tagged network traffic data (Liu et al., 2022, October).

CSE-CIC-IDS 2018: This dataset, which is intended to train models for identifying malware, DoS assaults, and botnets, contains a variety of cyberattack types, similar to CICIDS 2017 (Noever et al., 2021).

Kaggle Malware Dataset: The Android and Windows malware samples in the Kaggle dataset are frequently utilized in the industry for a variety of malware detection models, including mobile malware detection (Giovagnini, 2023).

Table 5.
Malware Datasets

Dataset Name	Description	Domain
CICIDS 2017	Contains network traffic and various attack data	Network
CSE-CIC-IDS 2018	Diverse attack dataset for cybersecurity research	Network
Kaggle Malware Dataset	Malware samples from Android and Windows devices	Mobile/Windows

Table 6.
Feature Selection Methods

Methodology	Sub-models	Description
Filter Methods	Chi-square, Mutual Information	Uses statistical methods to select relevant features.
Wrapper Methods	Recursive Feature Elimination (RFE)	Uses machine learning models to evaluate subsets of features.
Embedded Methods	Lasso Regression, Decision Trees	Selects features during model training.

Machine Learning Methods ML approaches examine files and classify them as dangerous or safe according to their characteristics (Colangelo, 2023).

Support Vector Machines (SVM): Identifies the optimal hyperplane for data classification; utilized for malware detection file classification (Azeez et al., 2021, February).

Random Forest: A group of decision trees that enhances malware detection accuracy and manages big datasets (Dolesi et al., 2024).

5.2 K-Nearest Neighbors (KNN):

This method is helpful for datasets with consistent malware types since it classifies samples based on the majority class among nearby samples (Gopinath et al., 2023).

Table 7.
Machine Learning Methods

Methodology	Sub-models	Description
Support Vector Machine (SVM)	Classification	Classifies malware based on extracted features.
Random Forest	Ensemble Learning	Combines multiple decision trees for improved classification.
K-Nearest Neighbors (KNN)	Instance-based Learning	Classifies based on proximity to similar data points.

Techniques for Deep Learning

In order to extract intricate features from massive amounts of data, deep learning is being utilized more and more in malware detection (Vasan et al., 2020).

CNNs: Used for image-based analysis, including feature extraction from unprocessed byte sequences (Rhode et al., 2018). System call logs and other sequence data are best suited for RNNs (Zahoora et al., 2022).
Auto-encoders: Learn typical program behavior to identify abnormalities (Kalphana et al., 2024).

Table 8.
Deep Learning Methods

Methodology	Sub-models	Description
Convolutional Neural Networks (CNNs)	Image-based analysis, Feature extraction	Learns patterns from images or raw byte sequences.
Recurrent Neural Networks (RNNs)	Sequence modeling, Malware behavior analysis	Analyzes sequential data, such as system call logs.
Auto encoders	Anomaly detection, Unsupervised learning	Identifies anomalies by learning normal data patterns.

HybridModels

Combining many methods lowers false positives and improves detection accuracy (Gao et al., 2023).
CNN + RNN: combines sequential analysis and feature extraction for raw data and behavior(Huda et al., 2019).
malware (Manthena, 2022), With their combined strengths,
5.3.3 Random Forest and DNNs offer precise and comprehensible malware detection (Dhillon, 2021).

Table 9.
Hybrid Models

Hybrid Approach	Components	Description
CNN + RNN	Convolutional Neural Networks + Recurrent Neural Networks	Combines CNNs for feature extraction and RNNs for sequence analysis.
SVM + K-Means	Support Vector Machine + K-Means Clustering	SVM for classification and K-Means for clustering similar malware.
Random Forest + DNNs	Random Forest + Deep Neural Networks	Combines interpretability of Random Forest with deep learning's power.

Using Transfer Learning to Identify Malware

Transfer learning detects new, undetected malware with little further training by using pre-trained models on huge datasets (Kumar, 2021).
Adjusting Pre-trained Models: Modifies a pre-trained model's final layers using sparse data (Bhardwaj et al., 2024).
Domain adaptation is the process of fine-tuning information from one domain (like Windows malware) to another (like Android) (Ali et al., 2022).

Multi-task learning improves the ability to recognize new malware by training on several malware kinds at once (Qureshi et al., 2024).

Table 10.
Transfer Learning Techniques

Transfer Learning Approach	Sub-models	Description
Fine-tuning Pre-trained Models	Fine-tuning, Adaptation	Adapts pre-trained models for new malware tasks.
Domain Adaptation	Cross-domain learning, New malware detection	Adapts models to detect new, unseen malware strains.
Multi-task Learning	Simultaneous learning, Multi-category detection	Trains models to detect multiple malware categories.

Metrics of Evaluation

Several metrics evaluate the accuracy and dependability of malware detection systems (Du et al., 2018)

Table 11.
Evaluation Metrics

Metric	Description
Accuracy	Measures overall correctness of the detection model.
Precision	Proportion of correct positive predictions.
Recall	Proportion of true positives correctly identified.
F1-score	Harmonic mean of precision and recall.
False Positive Rate (FPR)	Rate of benign instances misclassified as malware.
False Negative Rate (FNR)	Rate of malware misclassified as benign.

How effective are existing artificial intelligence approaches in detecting and mitigating malware?

By efficiently detecting novel and intricate malware patterns through adaptable, data-driven analysis, AI techniques like ML and DL improve antivirus automation—even in the absence of prior threat knowledge.

Supervised Learning: Identifies known malware based on behavior using labeled data (e.g., SVM, Random Forest).

Unsupervised Learning: When labels are not provided, this method (such as DBSCAN) finds anomalies in unlabeled data.

Deep Learning: Perfect for high-dimensional malware data, this technique learns hierarchical characteristics from raw data (e.g., CNNs, RNNs).

COMPARISON OF THE EXISTING LITERATURE WITH OUR STUDIES

Table 22.
Summary and Comaprison of our study with literature

	Malware Sophistication	Static & Dynamic Analysis	Malware Datasets	Feature Selection	ML & DL Results	Challenges	Hybrid Models	Transfer Learning
(Shaukat et al., 2020)	x	x	≈	x	✓	✓	x	x

(Or-Meir et al., 2019)		x	≈	x	x	x	x	x
(Ijiga et al., 2024)	≈		≈	≈	≈	✓	x	x
(Caviglione et al., 2020)	≈	x	x	≈	≈	≈	x	x
This article	✓	✓	✓	✓	✓	✓	✓	✓

Covered ✓; Partially Covered ≈; Not Covered x.

DISCUSSION

Because they can efficiently identify both linear and nonlinear patterns in complex high-dimensional data, AI techniques like Auto encoder, CNNs, and LSTMs are widely used for malware detection.

Ai-Based Models In Malware Detection

Auto encoders help handle partial or evasive malware data by recovering corrupted data. By recognizing important characteristics, CNNs enhance classification and aid in the detection of novel threats. LSTMs are excellent at identifying persistent malware behavior by examining sequential data, such as network traffic. Despite their benefits, these AI methods also come with some drawbacks, including high resource usage, long training periods, and a tendency to overfit, particularly when working with large datasets. Additionally, the interpretability of AI models, especially in deep learning techniques like CNNs and LSTMs, remains a significant challenge, as these models are often seen as "black boxes." This lack of interpretability can hinder the adoption of AI models in cybersecurity, where understanding the reasoning behind decisions is essential. While AI methods outperform traditional methods in handling complex malware datasets, there are still situations where traditional methods, like static analysis and rule-based detection, may be effective for simpler malware cases. In practice, combining AI-based approaches with traditional methods, such as static & dynamic analysis, may offer a more robust solution to malware detection, leveraging the strengths of both approaches.

LIMITATIONS OF THE STUDY

This SLR provides insightful information about AI-based malware detection, but it has limitations: it only included English articles; it only included peer-reviewed journal and conference papers, excluding non-peer sources; and it covered studies from 2015–2024, potentially missing the most recent developments. Future studies might uncover more developing techniques. This SLR emphasizes the efficacy of AI approaches such as AE, CNN, LSTM, and transfer learning in identifying new and elusive malware, particularly when used with conventional analysis tools. Real-time detection presents a number of difficulties, such as the requirement for high-quality data, processing demands, and model interpretability.

FUTURE DIRECTIONS

Future studies on AI-driven malware detection should concentrate on real-time detection on devices with limited resources, hybrid models that combine AI and conventional techniques, and extending transfer learning to better adapt to new threats and sparse data.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Afianian, A., Niksefat, S., Sadeghiyan, B., & Baptiste, D. (2019). Malware dynamic analysis evasion techniques: A survey. ACM Computing Surveys (CSUR), 52(6), 1-28.

Akhtar, M. S., & Feng, T. (2022). Detection of malware by deep learning as CNN-LSTM machine learning techniques in real time. Symmetry, 14(11), 2308.

Ali, R., Ali, A., Iqbal, F., Hussain, M., & Ullah, F. (2022). Deep learning methods for malware and intrusion detection: A systematic literature review. Security and Communication Networks, 2022(1), 2959222.

Ali, S., Abusabha, O., Ali, F., Imran, M., & Abuhmed, T. (2022). Effective multitask deep learning for iot malware detection and identification using behavioral traffic analysis. IEEE Transactions on Network and Service Management, 20(2), 1199-1209.

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. Applied sciences, 11(18), 8383.

Atitallah, S. B., Driss, M., & Almomani, I. (2022). A novel detection and multi-classification approach for IoT-malware using random forest voting of fine-tuning convolutional neural networks. Sensors, 22(11), 4302.

Azeez, N. A., Odufuwa, O. E., Misra, S., Oluranti, J., & Damaševičius, R. (2021, February). Windows PE malware detection using ensemble learning. In Informatics (Vol. 8, No. 1, p. 10). MDPI.

Bhardwaj, S., Li, A. S., Dave, M., & Bertino, E. (2024). Overcoming the lack of labeled data: Training malware detection models using adversarial domain adaptation. Computers & Security, 140, 103769.

Bruna Moralejo, L. (2023). Machine Learning for malware detection and classification (Master's thesis, Universitat Politècnica de Catalunya).

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. Ieee Access, 10, 93575-93600.

Caviglione, L., Choraś, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M., & Wasielewska, K. (2020). Tight arms race: Overview of current malware threats and trends in their detection. IEEE Access, 9, 5371-5396.

Chakkaravarthy, S. S., Sangeetha, D., & Vaidehi, V. (2019). A survey on malware analysis and mitigation techniques. Computer Science Review, 32, 1-23.

Colangelo, M. L. (2023). Malware family classification with semi-supervised learning (Doctoral dissertation, Politecnico di Torino).

Daniele Ucci, Leonardo Aniello, and Roberto Baldoni. 2019. Survey of machine learning techniques for malware analysis. Comput. Secur. 81 (2019), 123. DOI: https://doi.org/10.1016/j.cose.2018.11.001

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 15, 277-305.

De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). Artificial intelligence and the future of defense: strategic implications for small-and medium-sized force providers. The Hague Centre for Strategic Studies.

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

Demetrio, L., Coull, S. E., Biggio, B., Lagorio, G., Armando, A., & Roli, F. (2021). Adversarial exemples: A survey and experimental evaluation of practical attacks on machine learning for windows malware detection. ACM Transactions on Privacy and Security (TOPS), 24(4), 1-31.

Dhillon, H. (2021). Building effective network security frameworks using deep transfer learning techniques (Master's thesis, The University of Western Ontario (Canada)).

Diro, A., Chilamkurti, N., Nguyen, V. D., & Heyne, W. (2021). A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors, 21(24), 8320.

Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. Symmetry, 15(3), 677.

Dolesi, K., Steinbach, E., Velasquez, A., Whitaker, L., Baranov, M., & Atherton, L. (2024). A machine learning approach to ransomware detection using opcode features and k-nearest neighbors on windows. Authorea Preprints.

Du, P., Sun, Z., Chen, H., Cho, J. H., & Xu, S. (2018). Statistical estimation of malware detection metrics in the absence of ground truth. IEEE Transactions on Information Forensics and Security, 13(12), 2965-2980.

Dukarm, C. (2020). Mobile Data Analysis using Dynamic Binary Instrumentation and Static Analysis.

El-Shafai, W., Almomani, I., & AlKhayer, A. (2021). Visualized malware multi-classification framework using fine-tuned CNN-based transfer learning models. Applied Sciences, 11(14), 6446.

Farooq, U. (2023). Cyber-physical security: AI methods for malware/cyber-attacks detection on embedded/IoT applications (Doctoral dissertation, Politecnico di Torino).

Farooq, U. (2023). Cyber-physical security: AI methods for malware/cyber-attacks detection on embedded/IoT applications (Doctoral dissertation, Politecnico di Torino).

Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., ... & Wu, F. (2021, December). Malware detection and prevention using artificial intelligence techniques. In 2021 IEEE international conference on big data (big data) (pp. 5369-5377). IEEE.

Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems, 70, 447-489.

Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems, 70, 447-489.

Gaber, M. G., Ahmed, M., & Janicke, H. (2024). Malware detection with artificial intelligence: A systematic literature review. ACM Computing Surveys, 56(6), 1-33.

Gao, G., Wang, C., Wang, J., Lv, Y., Li, Q., Ma, Y., ... & Chen, G. (2023). CNN-Bi-LSTM: A complex environment-oriented cattle behavior classification network based on the fusion of CNN and Bi-LSTM. Sensors, 23(18), 7714.

Geenens, P. (2019). IoT Botnet Traits and Techniques: A View of the State of the Art. Botnets, 101-164. . Journal of Network and Computer Applications, 153, 102526.

Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges

Giovagnini, F. (2023). Interpretable Machine Learning for malware characterization and identification (Doctoral dissertation, Politecnico di Torino).

Gopinath, M., & Sethuraman, S. C. (2023). A comprehensive survey on deep learning based malware detection techniques. Computer Science Review, 47, 100529.

Hassen, M., Carvalho, M. M., & Chan, P. K. (2017, November). Malware classification using static analysis based features. In 2017 IEEE symposium series on computational intelligence (SSCI) (pp. 1-7). IEEE.

Huda, S., Abawajy, J., Al-Rubaie, B., Pan, L., & Hassan, M. M. (2019). Automatic extraction and integration of behavioural indicators of malware for protection of cyber–physical networks. Future generation computer systems, 101, 1247-1258.

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention.

Illes, D. (2022). On the impact of dataset size and class imbalance in evaluating machine-learning-based windows malware detection techniques. arXiv preprint arXiv:2206.06256.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2022). Enabling flexible manufacturing system (FMS) through the applications of industry 4.0 technologies. Internet of Things and Cyber-Physical Systems, 2, 49-62.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 564-574.

Kalphana, K. R., Aanjankumar, S., Surya, M., Ramadevi, M. S., Ramela, K. R., Anitha, T., ... & Krishnaraj, R. (2024). Prediction of android ransomware with deep learning model using hybrid cryptography. Scientific Reports, 14(1), 22351..

Karbab, E. B., & Debbabi, M. (2021). Resilient and adaptive framework for large scale android malware fingerprinting using deep learning and NLP techniques. arXiv preprint arXiv:2105.13491.

Koroniotis, N. (2020). Designing an effective network forensic framework for the investigation of botnets in the Internet of Things (Doctoral dissertation, UNSW Sydney).

Kumar, S. (2021). MCFT-CNN: Malware classification with fine-tune convolution neural networks using traditional and transfer learning in Internet of Things. Future Generation Computer Systems, 125, 334-351.

Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 9(20), 4396.

Liu, L., Engelen, G., Lynar, T., Essam, D., & Joosen, W. (2022, October). Error prevalence in nids datasets: A case study on cic-ids-2017 and cse-cic-ids-2018. In 2022 IEEE Conference on Communications and Network Security (CNS) (pp. 254-262). IEEE.

Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR), 54(5), 1-36.

Lwakatare, L. E., Raj, A., Crnkovic, I., Bosch, J., & Olsson, H. H. (2020). Large-scale machine learning systems in real-world industrial settings: A review of challenges and solutions. Information and software technology, 127, 106368.

Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2022). MalDetConv: automated behaviour-based malware detection framework based on natural language processing and deep learning techniques. arXiv preprint arXiv:2209.03547.

Manthena, H. (2022). Explainable machine learning based malware analysis (Master's thesis, North Carolina Agricultural and Technical State University).

Mehta, R., Jurečková, O., & Stamp, M. (2024). A natural language processing approach to Malware classification. Journal of Computer Virology and Hacking Techniques, 20(1), 173-184.

Mimura, M., & Ito, R. (2022). Applying NLP techniques to malware detection in a practical environment. International Journal of Information Security, 21(2), 279-291.

Minhaj, S. M. U. H. (2023). Study of artificial intelligence in cyber security and the emerging threat of AI-driven cyber attacks and challenge. Available at SSRN 4652028.

Noever, D., & Noever, S. E. M. (2021). Virus-MNIST: A benchmark malware dataset. arXiv preprint arXiv:2103.00602.

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), 1-48.

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), 1-48.

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), 1-48.

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access, 12, 12229-12256.

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access, 12, 12229-12256.

Pirscoveanu, R. S., Hansen, S. S., Larsen, T. M., Stevanovic, M., Pedersen, J. M., & Czech, A. (2015, June). Analysis of malware behavior: Type classification using machine learning. In 2015 International conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-7). IEEE.

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., ... & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. Journal of King Saud University-Computer and Information Sciences, 102164..

Raff, E., & Nicholas, C. (2020). A survey of machine learning methods and challenges for windows malware classification. arXiv preprint arXiv:2006.09271.

Review, taxonomy, and open research issues. Journal of Information Security and Applications, 55, 102582.

Rhode, M., Burnap, P., & Jones, K. (2018). Early-stage malware prediction using recurrent neural networks. computers & security, 77, 578-594.

Sarker, I. H. (2021). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. SN computer science, 2(6), 420.

Shafiq, U., Shahzad, M. K., Anwar, M., Shaheen, Q., Shiraz, M., & Gani, A. (2022). [Retracted] Transfer Learning Auto-Encoder Neural Networks for Anomaly Detection of DDoS Generating IoT Devices. Security and Communication Networks, 2022(1), 8221351.

Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., & Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments:

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE access, 8, 222310-222354.

Stiawan, D., Idris, M. Y. B., Bamhdi, A. M., & Budiarto, R. (2020). CICIDS-2017 dataset feature analysis with information gain for anomaly detection. IEEE Access, 8, 132911-132921.

Xu, X., Wang, Q., Li, H., Borisov, N., Gunter, C. A., & Li, B. (2021, May). Detecting ai trojans using meta neural analysis. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 103-120). IEEE.

Yan, P., & Yan, Z. (2018). A survey on dynamic mobile malware detection. Software Quality Journal, 26(3), 891-919.

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.

Yudkowsky, E. (2008). Artificial intelligence as a positive and negative factor in global risk. Global catastrophic risks, 1(303), 184.

Yunmar, R. A., Kusumawardani, S. S., & Mohsen, F. (2024). Hybrid Android Malware Detection: A Review of Heuristic-Based Approach. IEEE Access, 12, 41255-41286.

Zahoora, U., Rajarajan, M., Pan, Z., & Khan, A. (2022). Zero-day ransomware attack detection using deep contractive autoencoder and voting based ensemble classifier. Applied Intelligence, 52(12), 13941-13960

2025 by the authors; The Asian Academy of Business and social science research Ltd Pakistan. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).