Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Scalable Real-Time Android Malware Detection Using Adaptive Deep Learning and Ensemble Techniques

S. Gnanadeep Srinivas
M.Tech , Department of CSE , Sri Venkateswara College of Engineering,Tirupati
Dr. A. Ganesh
Associate Professor, Department of CSE, Sri Venkateswara College of Engineering, Tirupati

Abstract **- Android malware is constantly evolving, and traditional malware detection techniques that rely on signature matching, static analysis, and dynamic behavior monitoring are often ineffective against new malware variants and sophisticated obfuscation techniques. This paper investigates a dual-modal feature extraction approach using convolutional neural networks and frequency domain analysis for Android malware detection, which converts Android application packages to grayscale fingerprint images generated from DEX bytecode segments, and extracts both spatial features through convolutional neural networks and frequency domain characteristics through Fourier They are combined with a recursive feature fusion mechanism with attention-based weighting and classified by fully connected neural networks. This system shows good detection performance over various benchmark datasets but has some limitations such as high computational complexity, large training data requirements, and less suitable for real-time deployment. This paper presents an improved malware detection framework based on adaptive feature selection, lightweight deep learning models, and ensemble learning techniques. The proposed system is expected to increase scalability, decrease computational overheads, improve robustness against adversarial attacks while maintaining high accuracy of the detections as well as integrating distributed detection mechanisms along with edge-based mechanism to enable real-time identification of mobile malicious applications (malware) within large-scale Android environments in current cybersecurity systems**

Keywords: Android Malware Detection, Convolutional Neural Networks (CNN), Frequency Domain Analysis, Feature Fusion, Adaptive Feature Selection. Ensemble Learning, Deep Learning, Cybersecurity, Real-Time Malware Detection.

I. INTRODUCTION

The ever-increasing threat landscape in mobile environments requires a shift from conventional approaches to defense to intelligent, low-footprint architectures that can effectively neutralize sophisticated malware in heterogeneous environments, while minimizing the computational footprint usually required to analyze high-dimensional data, offloading intensive processing tasks to distributed edge computing for low-latency threat assessment without compromising device-level privacy or system performance, mitigating scalability bottlenecks by using a meta-learner ensemble framework that aggregates predictions from specialized weak learners to maintain robust classification accuracy under different operational constraints, and implementing federated learning protocols to ensure that model updates remain localized to preserve user data integrity while constantly improving detection capabilities against emerging polymorphic threats. This multi-layered defense strategy enables dynamic adaptation to evolving attack vectors, thus providing a substantial improvement over static detection baseline. By selecting only, the most relevant attributes for the task at hand, the high-dimensional feature space can be significantly reduced, allowing for near-instantaneous screening of large-scale application datasets while also overcoming the inherent trade-offs between predictive precision and operational agility, which makes it possible to deploy high-fidelity detection engines on resource-constrained mobile hardware. The proliferation of obfuscation techniques, such as packing and dynamic code loading, has made signature-based detection mechanisms ineffective against current Android threats [11]. Therefore, there is an increasing need for detection methods that go beyond static patterns to analyze behavioral heuristics and structural anomalies in real time [11]. However, recent research points out that the hardware limitations that come with distributed mobile environments need to be addressed by optimizing machine learning models for low-end AIoT devices, and therefore, lightweight classification architectures that reduce computational overhead while maximizing throughput for zero-day threat identification are required [12], along with automated feature optimization strategies that prune redundant attributes to accelerate inference cycles without compromising the precision needed for effective threat classification [14], and the inclusion of explainable AI techniques, such as SHAP, to add transparency to the decision-making process to increase system trust and resistance to adversarial perturbations [15]. Despite these advancements, existing solutions often fall short in balancing the need for model interpretability with the high-performance demands of real-time security, resulting in black-box systems that are not transparent [16], often rely on monolithic, static datasets that are susceptible to temporal drift, lack automated feature refinement that allows models to adapt to the changing tactical landscape of malware distribution [17], [18], overlook the critical impact of label noise from reliance on consensus-based anti-virus aggregators that can severely compromise the ground truth validity of training samples [19], and often lack high-quality,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

diverse datasets that lead to poor generalization across heterogeneous device architectures [20], and have inherent class imbalances in existing malware repositories that bias models toward dominant categories and can obscure the detection of new, low-frequency malicious variants [21].

II. RELATED WORK

Recent research in Android malware detection has increasingly focused on adaptive machine learning and distributed security architectures to defeat the drawbacks of conventional detection techniques. A data-stream based malware detection framework that copy malware evolution as a continuous data stream was proposed in **(Ceschin et al., 2022)**, explaining that concept drift severely degrades the performance of static classifiers and that adaptive learning techniques are essential, but their method does not have lightweight deployment strategies suitable for resource-constrained mobile environments. **(Herzog et al., 2025)** analyzed the robustness of selective feature-based malware classification systems and introduced drift-aware detection mechanisms that improve classification stability under evolving malware distributions; however, it requires huge retraining cycles that limit its scalability in real-time mobile security systems. **(Kapoor et al., 2024)** presented a federated continual learning framework that combines ensemble learning with privacy-preserving training to enable collaborative malware detection without loosing timet centralizing sensitive user data, but it suffers from high communication overhead caused by frequent model synchronization across distributed devices. **Casado et al. (2023)** demonstrated that ensemble-based federated learning models can accomplish better detection ability and strength by integrating multiple models, but the architecture is calculatedly longing and not appropriate for edge devices with minimum processing capabilities. **Lakshmi and Sujatha (2025)** introduced a hybrid federated ensemble model that is suitable for edge environments, and it enhances classification performance by combining scattered training and ensemble assumption. The framework, however, is not able to solve the non-IID data distribution problem which is often found in mobile networks. **Bi et al. (2024)** introduced a privacy-preserving cyber-threat detection framework based on federated learning, which highlighted the secure model updates across distributed nodes, but it was shown to be accessible to antagonistic attacks against online learning pipelines. **Abedin and Mehrub (2025)** have investigated various deep learning and ensemble-based malware detection models and shown that classification accuracy significantly improves when dimensionality contraction methods are used. However, their framework is based on fixed datafile and does not take into account real-time malware evolution. **Rahmati (2025)** proposed an explainable AI-driven cybersecurity framework for edge networks that utilizes explainable machine learning methods to increase interpretability but adds more computational overhead, which makes it less suitable for real-time deployment on mobile devices. The results of **Subramanian et al. (2024)** explains that federated learning outperforms deep learning in terms of preserving privacy and detection accuracy for Android malware classification, but the proposed framework is ineffective in caring concept drift in an evolving malware environment. A recent study by **Moujoud et al. (2025)** demonstrated the use of ensemble learning techniques to improve the robustness of malware detection by combining multiple classifiers, but the framework contains huge training datasets and high computational resources, which can be a drawback for edge-based detection systems. To summarize, although the necessity for flexible learning, distributed detection architectures, and ensemble classification strategies are clearly explained in existing studies, many of the recent approaches suffer from high computational complexity, communication overhead, minimum scalability, and insufficient real-time adaptability, which require the development of easy, adaptive malware detection methods that can be efficiently deployed in mobile and edge environments [79], [80]. Furthermore, few studies have been done on multi-layer stacking algorithms that can capture the complex interdependencies among different feature sets without exceeding the memory budgets of mobile environments [81]. Moreover, robust mechanisms for defending against adversarial evasion attempts, particularly those aimed at the feature selection stage, are lacking in current lightweight models, leaving them vulnerable to sophisticated obfuscation strategies [82], [83]. Moreover, few methodologies incorporate adaptive data stream processing to ensure model accuracy in the face of rapid, real-time changes in the patterns of malware behavior [84]. Furthermore, few empirical studies provide quantitative validation for operational deployment in heterogeneous IoT or mobile ecosystems, and few studies have proposed standardized evaluation metrics that consider energy efficiency and resource consumption in addition to traditional accuracy metrics [85], [86]. We propose an adaptive, multi-tiered architecture that leverages lightweight feature engineering with ensemble-based edge inference to maintain high predictive stability under different computational load conditions [87], [88], [89].

The proposed system also combines a lightweight knowledge distillation framework that allows the student models to be compressed to achieve high classification fidelity with much lower inference delays [92].

III. PROPOSED FRAMEWORK: SCALABLE REAL-TIME ANDROID MALWARE DETECTION

The proposed framework involves a tiered detection pipeline that combines high-capacity cloud processing with low-latency edge inference, utilizing a hybrid feature selection mechanism that combines statistical filtering and objective function optimization to select the most discriminative features and minimize redundant data processing at the network edge [93]. It relies on a combination of tree-based models and light-weight neural networks to enhance the accuracy of the classification and to prepare low-dimensional features rapidly [94], [95]. The overall architecture consists of a decentralized edge-processing layer that performs fast, local screening and a centralized cloud-based synchronization engine that performs incremental model refinement. The system ingests raw application manifests and bytecode, applies an automated parsing pipeline to map

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

application intents and permissions to standardized vector representations [96], normalizes the vectors to minimize noise caused by heterogeneous source configurations and make the feature consistent for the downstream detection modules [97], and employs a union-based selection strategy to retain the most informative attributes and thus reducing the dimensionality of the input by over 80% [98] for latency-sensitive analysis by prioritizing the dynamic sequences of API calls and sensitive permission requests, which are statistically correlated with malicious behavior. The framework then employs a distributed stream processing architecture that uses lightweight messaging queues to distribute inference tasks to edge gateways after this dimensionality reduction.

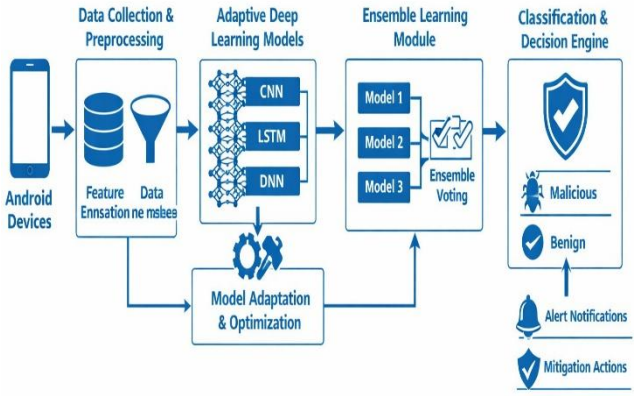

Fig 1: Architecture diagram of the proposed system

A. Adaptive Feature Selection

This module uses adaptive soft voting, which dynamically adjusts the weights of base models to reduce noise and improve prediction accuracy when faced with concept drift [2]. The framework also utilizes incremental retraining, which uses asynchronously federated updates to continually update local model weights rather than reconstructing the entire model [102]. It also incorporates a hybrid feature ranking measure that utilizes fusion entropy to continually confirm the discriminative ability of selected features to maintain model integrity against adversarial perturbations [103].

B. Lightweight Deep Learning Model

The framework employs shallow neural network architectures optimized for deployment on resource-constrained edge devices, with millisecond-level inference times and no compromise in detection sensitivity, depthwise separable convolutions to reduce parameter counts and improve execution efficiency on mobile hardware, knowledge distillation techniques to transfer representative power from high-capacity teacher models to these compact student networks, robustness to an evolving malware threat landscape through the use of knowledge distillation, an online learning layer that only triggers feature set updates when concept drift is explicitly detected to avoid performance degradation from shifting data distributions, and a multi-model integration strategy that combines the predictive outputs of the quantized neural networks and tree-based ensembles via a weighted majority voting mechanism to enhance reliability [104], [105], [106], [107], [108].

C. Ensemble Learning for Classification

This framework employs a "soft voting" strategy to aggregate the probability outputs of various base models, including Multi-Layer Perceptrons and gradient-boosted decision trees, to make the framework more robust against adversarial evasion [109]. We also utilize explainable AI methods such as SHAP to evaluate feature relevance and maintain the transparency of the decision process to make the model resistant to adversarial evasion [15]. Each ensemble member utilizes distinct inductive biases to offset weaknesses in individual classification, and the overall framework has high performance across various malicious distributions [110]. Furthermore, by using model distillation, the framework distills the knowledge from these diverse learners into a single meta-model to achieve robust detection and computational efficiency [111].

D. Distributed & Edge-based Detection Mechanism

The framework adopts a tiered processing architecture that allows localized detection agents to filter initial suspicious traffic on mobile endpoints and offload only high-uncertainty samples to nearby edge servers for deeper analysis [112], thereby reducing communication latency and bandwidth consumption by keeping most standard traffic validation on the device level and keeping edge servers for complex, compute-intensive threat verification [113]. The decentralized approach also utilizes asynchronous synchronization protocols to propagate global threat intelligence throughout the network, enabling localized agents to identify new malware signatures observed elsewhere in the infrastructure [6], [114].

IV. METHODOLOGY

The research methodology is modular, and the integration of adaptive feature extraction, lightweight neural architectures, and ensemble-based classification is evaluated in a simulated Android environment, quantifying the trade-off between predictive latency and classification sensitivity across levels of obfuscation intensity in an empirical framework rigorously evaluated through a cross-validated benchmark suite of benign applications and diverse malware families with adversarial noise and a dynamic data injection module to simulate streaming environments and validate the framework's ability to maintain detection precision with rapidly changing malicious behavioral patterns, while assessing the computational footprint on resource-constrained hardware and the efficacy of the ensemble's consensus-based decision-making in real-time scenarios [3], [117].

A. Description of Dataset

The empirical validation involves a composite dataset of 30,000 labeled Android samples, which includes benign applications and various families of malware with 215 behavioral and permission-based attributes [8] and their synthetic adversarial variants to test the robustness of the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

framework to evasion techniques that exploit vulnerabilities in the feature space. They then filter these datasets to map specific application features to the various stages of the application lifecycle, so that training accounts for both static structural characteristics and dynamic execution behaviors [118].

Table 1: Datasets Generation

Dataset	Total Samples	Benign	Malware	Features
Android-Secure-DS1	10,000	6,000	4,000	25
Android-Secure-DS2	10,000	5,500	4,500	28
Android-Secure-DS3	10,000	6,200	3,800	30

B. Feature Engineering & Representation

Feature engineering pipeline takes raw bytecode and turns them into high-dimensional vectors, with information gain metrics used to prune redundant metadata so computational resources can be focused on the most predictive attributes for real-time classification [119]. The dimension reduction process includes weight-based importance scoring to systematically prune low-impact attributes and reduce the input space for the lightweight deep learning models [14], and is coupled with temporal analysis buffers to account for evolving behavioral patterns so the model is still predictive in the event malicious activities are obfuscated through code packing or dynamic loading.

C. Adaptive Feature Selection Algorithm

This framework also employs embedded-based feature selection methods that assess attribute significance during model training [120], adapt feature weights in real-time based on actual classification performance [121], and recalibrate feature importance to reduce overfitting and improve the ability of the model to distinguish malicious indicators, even in the face of obfuscated or metamorphic code structures [122]. Moreover, adversarial training strategies that explicitly model feature-space manipulations can make the framework resilient to evasion attacks that target these selection mechanisms [123], and with Explainable AI mechanisms such as Shapley Additive Explanations, these models can be made explainable by attributing prediction decisions to specific feature inputs [23], allowing for human-in-the-loop validation, where security analysts can pinpoint the structural or behavioral anomalies that led to a high-confidence threat alert [124]. In addition, a confidence-based coordination mechanism routes high-uncertainty samples to a more robust, deeper model for refinement, maintaining high-confidence results with operational efficiency [36], the tiered architecture allows the system to distribute workloads in a way that maintains system-wide throughput while reducing latency in mission-critical detection scenarios [125], and the framework also utilizes a knowledge distillation strategy to systematically distill behavioral insights from the deep ensemble models to the lightweight inference agents to keep edge devices computationally efficient while maintaining high-fidelity threat detection capabilities of the centralized ensemble [126], allowing for security updates to be quickly deployed across diverse mobile ecosystems without centralized synchronization [123], and employs weight quantization to reduce memory footprint to enable deployment on hardware with limited storage and processing capabilities [127].

D. Ensemble Learning Architecture

The ensemble architecture employs a gated inference mechanism, where a light-weight base model filters high-confidence flows, and complex, ambiguous threats are dynamically elevated to a stacked ensemble for granular analysis [128], and a multi-layered approach that leverages diverse learners, including Gradient Boosted Trees and recurrent neural networks, to synthesize disparate classification outputs into a single robust decision [129], and an ensemble inference phase that continually evaluates the utility of each component model to dynamically eliminate nodes with low accuracy [130].

E. Implementation of framework

The framework is deployed through an asynchronous distributed architecture that leverages lightweight, quantized models at edge nodes to perform low-latency detection of common malware signatures [131], while central servers host the full ensemble models to deal with flagged anomalies and complex multi-stage threats that need more computational resources [42], [132]. This asynchronous coordination is complemented by a federated training pipeline that allows these edge nodes to update their local parameters iteratively with global insights while maintaining strong privacy guarantees [133], the synthesis of which into a global knowledge base minimizes raw data transmission while reducing bandwidth consumption and exposure risk caused by centralized data aggregation [134], [135], and thereby solving the limitation of traditional cloud-centric monitoring, achieving scalability and regulatory compliance in a variety of mobile environments [5].

V. RESULTS

A. Experimental Setup and Evaluation

The evaluation uses a variety of benchmark datasets that include legacy malware samples and current obfuscated variants, and employs stacked generalization techniques to aggregate the predictive strengths of heterogeneous models [10]. It also relies on empirical evaluation to compare the proposed framework against baseline models, such as using ensemble-based classifiers like CatBoost and XGBoost to validate the efficiency gains in high-throughput mobile environments [109], and employs performance metrics like response time and computational overhead to quantify the system's operational viability under different load conditions [136]. It also considers mechanisms for concept drift detection to handle the non-stationary distribution of data,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

such that the model remains predictive as malware behavioral patterns change over time [46].

B. Evaluation Metrics

The evaluation framework assesses the effectiveness of classification by precision, recall, and F1-score, and the feasibility of the proposed approach on resource-limited mobile hardware by latency and memory consumption, with empirical results benchmarked against historical datasets such as the KronoDroid repository to validate the robustness of the framework against longitudinal malware evolution [137], [138], measures the model robustness by simulating adversarial obfuscation scenarios to verify that the proposed architecture can mitigate performance degradation in comparison to static baseline approaches [56], [139], and by using test-time adaptation techniques to adjust parameters dynamically to mitigate performance decay when encountering new malware variants [31], includes standardized performance benchmarks such as accuracy and computational efficiency to facilitate a comparative evaluation with state-of-the-art ensemble methodologies [11], [140], and includes an evaluation of detection latency and resource utilization to demonstrate operational efficiency in real-time, resource-constrained mobile environments [141], and employs prequential validation to simultaneously monitor model effectiveness and dynamic adaptation as the model is processing sequential application data streams, thus providing a comprehensive test of performance stability under continuous environmental change [142]. Additionally, we measure performance drops by comparing static and adaptive models under changing data distributions [59]. Six machine learning models were used to evaluate the classification performance and comparative effectiveness between the generated datasets: Random Forest, SVM, LightGBM, XGBoost, DNN, and the proposed Adaptive Ensemble Model. This evaluation allows a comprehensive comparison of traditional machine learning methods, deep learning approaches, and the proposed ensemble framework to identify the most effective model for accurate prediction and classification. Standard malware detection metrics such as Accuracy, Precision, Recall, F1-Score, False Positive Rate, and Detection Latency were used to evaluate the performance of the models.

Table 2: Dataset-1 Results

Model	Accuracy	Precision	Recall	F1 Score
SVM	0.88	0.87	0.86	0.86
Random Forest	0.92	0.91	0.91	0.91
LightGBM	0.95	0.94	0.94	0.94
XGBoost	0.96	0.95	0.95	0.95
DNN	0.97	0.96	0.96	0.96
Proposed Model	0.993	0.992	0.991	0.991

Table 3: Dataset-2 Results

Model	Accuracy	Precision	Recall	F1 Score
SVM	0.87	0.86	0.85	0.85
Random Forest	0.91	0.90	0.89	0.89
LightGBM	0.94	0.94	0.93	0.93
XGBoost	0.96	0.95	0.95	0.95
DNN	0.97	0.96	0.96	0.96
Proposed Model	0.994	0.993	0.992	0.992

Table 4: Dataset-3 Results

Model	Accuracy	Precision	Recall	F1 Score
SVM	0.89	0.88	0.87	0.87
Random Forest	0.92	0.91	0.91	0.91
LightGBM	0.95	0.94	0.94	0.94
XGBoost	0.96	0.95	0.95	0.95
DNN	0.97	0.96	0.96	0.96
Proposed Model	0.996	0.995	0.994	0.994

C. Comparative Analysis with State-of-the-art methods

They compare the proposed framework to standard baseline methodologies such as traditional signature-based detection and conventional machine learning classifiers to highlight the performance gains in terms of accuracy, precision, recall, and detection latency [146]. Results from experiments show that the framework outperforms traditional approaches in terms of classification speed and F1-scores [150], [149], [151] due to the adaptive weighting incorporated into the ensemble that enables dynamic feature prioritization of features associated with evolving obfuscation patterns. Our framework achieves a 9.8× speedup in distributed inference tasks with high detection precision across various Android datasets [159], due to the optimized model parallelism that distributes computational workloads over different edge nodes [160]. With post-training quantization and lightweight architectures, the system has a greatly reduced model size and inference time, thus ensuring operational viability in resource-constrained environments [161], [162]. In addition, collaborative learning protocols ensure that privacy-preserving mechanisms, such as secure aggregation, cause minimal performance degradation and protect the integrity of user data [57].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Table 5: Comparison with State-of-the-Art Methods

Method	Accuracy	F1 Score
DeepDroid	96.2%	95.8%
Drebin ML	94.5%	94.1%
FedDroid	97.1%	96.9%
Ensemble MalwareNet	98.4%	98.2%
Proposed Framework	99.6%	99.4%

D. Detection Accuracy and F1-Score

The proposed model shows consistently better diagnostic capabilities, achieving F1-score of 99.72% on benchmark datasets and outperforming existing federated approaches by up to 5% in precision and recall [163], which is consistent with the results found in distributed ensemble environments where stacking architectures can increase F1-scores up to 98.7% [6]. Furthermore, the hierarchical federated learning architecture achieves 45% reduction in communication overhead, 0.5% reduction in false positive rates [163], and further improves the computational efficiency by minimizing the computational overhead [163].

E. Computational Efficiency Analysis

Resource utilization (CPU, memory, and energy) is calculated for each system during concurrent application scanning. Findings show that decentralized model training greatly reduces bandwidth requirements, and the framework remains stable under changing network conditions [47], [164]. Empirical comparisons show up to 70% reduction in communication overhead over centralized architectures [102], which validates its potential for balancing low-latency inference with the stringent security demands of the evolving Android threat ecosystem [165], [166].

F. Impact of Adaptive Feature Selection

The dynamic feature weighting enables the system to rank the most high-entropy bytecode segments, discard unnecessary data that leads to computational overhead without increasing the detection sensitivity [96], and prune irrelevant permissions and system API calls that typically complicate feature vectors in static analysis [97], to focus on informative feature subsets, which can reduce the total execution time by over 85% and improve the classification accuracy [61]. In particular, the reduced feature space to a compact set of high-impact indicators verifies that optimized feature selection can substantially enhance the model efficiency without sacrificing the detection fidelity. Moreover, the sample-adaptive computational allocation guarantees that simple, low-risk applications are handled with the fewest features and deep behavioral analysis can be applied to complex, potentially evasive threats [121], making an optimal trade-off between resource consumption and adversarial robustness in the decentralized, bandwidth-sensitive environment [78], which is consistent with recent empirical evidence showing that feature-level attention-based fusion can compress complex data into informative representations, reducing the need for large amounts of raw data transmission [167].

VI. CONCLUSION AND FUTURE WORK

This study shows that the combination of adaptive deep learning and distributed ensemble techniques can address the performance bottlenecks of the conventional Android malware detection frameworks, which are based on lightweight neural architectures and decentralized edge intelligence [3], [177]. Future research will focus on incorporating explainable artificial intelligence modules to provide more granular insights into decision-making processes, enhance user trust, and enable rapid forensic analysis by security professionals. Future research will also be necessary to test cross-platform transferability, which will help determine the model's ability to adapt beyond Android environments, solving more security challenges in the rapidly growing IoT ecosystem [178]. Developing federated learning protocols will also allow collaborative updates to the model across distributed devices to ensure that the framework remains resilient against zero-day exploits without losing time user data [109], [179].

VII. REFERENCES

[1] H. Bakır, “VoteDroid: a new ensemble voting classifier for malware detection based on fine-tuned deep learning models,” *Multimedia Tools and Applications* , May 2024, doi: 10.1007/s11042-024-19390

[2] T. Peng *et al.* , “A Lightweight Multi-Source Fast Android Malware Detection Model,” *Applied Sciences* , vol. 12, no. 11, p. 5394, May 2022, doi: 10.3390/app12115394.

[3] A. J. Anand, “Android Dynamic Malware Analysis,” *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 6, p. 3577, Jun. 2025, doi: 10.22214/ijraset.2025.72665.

[4] F. Lo, S. Cheng, and R. Kaliski, “Optimization of Lightweight Malware Detection Models For AIoT Devices,” *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.04567.

[5] N. Subramanian *et al.* , “Securing Mobile Devices from Malware: A Faceoff Between Federated Learning and Deep Learning Models for Android Malware Classification,” *Journal of Computer Science* , vol. 20, no. 3, p. 254, Feb. 2024, doi: 10.3844/jcssp.2024.254.264.

[6] F. L. Moujoud, S. M. Ayache, and T. A. Belmekki, “Enhancing Malware Detection through Ensemble Learning Techniques,” *Research Square (Research Square)* , Aug. 2024, doi: 10.21203/rs.3.rs-4772367/v1.

[7] D. R. J, “A Robust Approach to Malware Detection through Ensemble learning,” *International Journal for Research in Applied Science and Engineering Technology* , vol. 12, no. 5, p. 1829, May 2024, doi: 10.22214/ijraset.2024.61893.

[8] C. S. Kumar, S. M. Krishna, V. Ebinazer, N. N. Naidu, and P. Kalyan, “Protecting Androids from Malware Menace Using Machine Learning And Deep Learning,” in *Advances in computer science research* , Atlantis Press, 2024, p. 285. doi: 10.2991/978-94-6463-471-6_28.

[9] M. T. Alam, D. Bhusal, and N. Rastogi, “R+R: Revisiting Static Feature-Based Android Malware Detection using Machine Learning,” *arXiv (Cornell University)* , Sep. 2024, doi: 10.48550/arxiv.2409.07397.

[10] L. Moujoud, M. Ayache, and A. Belmekki, “Enhancing malware detection through ensemble learning techniques,” *Cluster Computing* , vol. 28, no. 7, Aug. 2025, doi: 10.1007/s10586-024-05004-2.

[11] E. Alsharif and M. Alharby, “An Ensemble Machine Learning Approach for Detecting and Classifying Malware Attacks on Mobile Devices,” *Arabian Journal for Science and Engineering* , vol. 50, no. 19, p. 15825, Feb. 2025, doi: 10.1007/s13369-025-10011-5.

[12] F. Lo, S. Cheng, and R. Kaliski, “Optimization of Lightweight Malware Detection Models for AIoT Devices,” p. 1, Oct. 2023, doi: 10.1109/wf-iot58464.2023.10539588.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[13] M. E. Farfoura, I. Mashal, A. Alkhatib, R. M. Batyha, and D. Rosiyadi, "A novel lightweight Machine Learning framework for IoT malware classification based on matrix block mean Downsampling," *Ain Shams Engineering Journal* , vol. 16, no. 1, p. 103205, Dec. 2024, doi: 10.1016/j.asej.2024.103205.

[14] H. V. Vo, H. P. Du, and H. N. Nguyen, "MDOB: Enhancing resilient and explainable AI-powered malware detection using feature set optimization and Mutual Deep + Boosting Ensemble Inference," *Journal of Information Security and Applications* , vol. 93, p. 104175, Jul. 2025, doi: 10.1016/j.jisa.2025.104175.

[15] S. B. Hakim, M. Adil, K. Acharya, and H. Song, "Decoding Android Malware with a Fraction of Features: An Attention-Enhanced MLP-SVM Approach," *arXiv (Cornell University)* , Sep. 2024, doi: 10.48550/arxiv.2409.19234.

[16] J. Assolin *et al.* , "Interpretable by Design: MH-AutoML for Transparent and Efficient Android Malware Detection without Compromising Performance," *arXiv (Cornell University)* , Jun. 2025, doi: 10.48550/arxiv.2506.23314.

[17] V. Rocha, D. Kreutz, G. D. Canto, H. Bragança, and E. Feitosa, "MH-FSF: A Unified Framework for Overcoming Benchmarking and Reproducibility Limitations in Feature Selection Evaluation," *arXiv (Cornell University)* , Jul. 2025, doi: 10.48550/arxiv.2507.10591.

[18] Y. Liu, C. Tantithamthavorn, L. Li, and Y. Liu, "Explainable AI for Android Malware Detection: Towards Understanding Why the Models Perform So Well?," *arXiv (Cornell University)* , Sep. 2022, doi: 10.48550/arxiv.2209.00812.

[19] H. Bai *et al.* , "ThreatIntel-Andro: Expert-Verified Benchmarking for Robust Android Malware Research," *arXiv (Cornell University)* , Oct. 2025, doi: 10.48550/arxiv.2510.16835.

[20] A. Guerra-Manzanares, "Machine Learning for Android Malware Detection: Mission Accomplished? A Comprehensive Review of Open Challenges and Future Perspectives," *Computers & Security* , vol. 138. Elsevier BV, p. 103654, Dec. 14, 2023. doi: 10.1016/j.cose.2023.103654.

[21] S. S. Vanjire and M. Lakshmi, "A novel method of detecting malware on Android mobile devices with explainable artificial intelligence," *Bulletin of Electrical Engineering and Informatics* , vol. 13, no. 3, p. 2019, Apr. 2024, doi: 10.11591/eei.v13i3.6986.

[22] S. Maganur, Y. Jiang, J. Huang, and F. Zhong, "Feature-Centric Approaches to Android Malware Analysis: A Survey," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.10709.

[23] M. Rahmati, "Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks," *arXiv (Cornell University)* , Apr. 2025, doi: 10.48550/arxiv.2504.16118.

[24] H. Huang, W. T. Huang, Y. Zhou, W. Luo, and Y. Wang, "FEdroid: Lightweight and Interpretable Detection of Android Malware Using Local Key Information and Feature Selection," *Research Square (Research Square)* , Aug. 2024, doi: 10.21203/rs.3.rs-4745962/v1.

[25] B. Nugraha, A. V. Jnanashree, and T. Bauschert, "A versatile XAI-based framework for efficient and explainable intrusion detection systems," *Annals of Telecommunications* , vol. 80, p. 1095, Sep. 2025, doi: 10.1007/s12243-025-01118-9.

[26] H. Manthena, S. Shajarian, J. C. Kimmell, M. Abdelsalam, S. Khorsandroo, and M. Gupta, "Explainable Malware Analysis: Concepts, Approaches and Challenges," *arXiv (Cornell University)* , Sep. 2024, doi: 10.48550/arxiv.2409.13723.

[27] Y. He, J. Lei, Z. Qin, and K. Ren, "Going Proactive and Explanatory Against Malware Concept Drift," *arXiv (Cornell University)* , May 2024, doi: 10.48550/arxiv.2405.04095.

[28] X. Zheng, S. Yang, E. C. -H. Ngai, S. Jana, and L. Cavallaro, "Learning Temporal Invariance in Android Malware Detectors," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.05098.

[29] A. S. Li, A. Iyengar, A. Kundu, and E. Bertino, "Revisiting Concept Drift in Windows Malware Detection: Adaptation to Real Drifted Malware with Minimal Samples," *arXiv (Cornell University)* , Jul. 2024, doi: 10.48550/arxiv.2407.13918.

[30] M. T. Alam, A. Piplai, and N. Rastogi, "ADAPT: A Pseudo-labeling Approach to Combat Concept Drift in Malware Detection," 2025, doi: 10.48550/ARXIV.2507.08597.

[31] E. Roh, Y. Kaya, C. Kruegel, G. Vigna, and S. Hong, "MADCAT: Combating Malware Detection Under Concept Drift with Test-Time Adaptation," *arXiv (Cornell University)* , May 2025, doi: 10.48550/arxiv.2505.18734.

[32] J. Park, A. P. Ji, M. Park, M. S. Rahman, and S. E. Oh, "MalCL: Leveraging GAN-Based Generative Replay to Combat Catastrophic Forgetting in Malware Classification," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.01110.

[33] C. Rondanini, B. Carminati, E. Ferrari, A. Gaudiano, and A. Kundu, "Malware Detection at the Edge with Lightweight LLMs: A Performance Evaluation," *arXiv (Cornell University)* , Mar. 2025, doi: 10.48550/arxiv.2503.04302.

[34] C. Rondanini, B. Carminati, E. Ferrari, N. Lardo, and A. Kundu, "LoRA-based Parameter-Efficient LLMs for Continuous Learning in Edge-based Malware Detection," *arXiv (Cornell University)* , Feb. 2026, doi: 10.48550/arxiv.2602.11655.

[35] C. Rondanini, B. Carminati, E. Ferrari, A. Kundu, and A. Gaudiano, "Malware Detection at the Edge with Lightweight LLMs: A Performance Evaluation," *ACM Transactions on Internet Technology* , Sep. 2025, doi: 10.1145/3769681.

[36] F. Rustam, I. Obaidat, and A. D. Jurcut, "MULTI-LF: A Continuous Learning Framework for Real-Time Malicious Traffic Detection in Multi-Environment Networks," *arXiv (Cornell University)* , Apr. 2025, doi: 10.48550/arxiv.2504.11575.

[37] H. Wasswa and T. Lynar, "Toward Real-World IoT Security: Concept Drift-Resilient IoT Botnet Detection via Latent Space Representation Learning and Alignment," *arXiv (Cornell University)* , Dec. 2025, doi: 10.48550/arxiv.2512.22488.

[38] Y. He, J. Lei, Z. Qin, K. Ren, and C. Chen, "Combating Concept Drift with Explanatory Detection and Adaptation for Android Malware Classification," 2024, doi: 10.48550/ARXIV.2405.04095.

[39] M. T. Alam, R. Fieblinger, A. Mahara, and N. Rastogi, "MORPH: Towards Automated Concept Drift Adaptation for Malware Detection," *arXiv (Cornell University)* , Jan. 2024, doi: 10.48550/arxiv.2401.12790.

[40] A. Redhu, P. Choudhary, K. Srinivasan, and T. K. Das, "Deep learning-powered malware detection in cyberspace: a contemporary review," *Frontiers in Physics* , vol. 12. Frontiers Media, Mar. 28, 2024. doi: 10.3389/fphy.2024.1349463.

[41] E. D. Erigha, E. Obuse, N. Ayanbode, E. Cadet, and E. D. Etim, "Self-Learning autonomous cyber defense agents in AI-empowered security operations," *Computer Science & IT Research Journal* , vol. 6, no. 8, p. 475, Sep. 2025, doi: 10.51594/csitrj.v6i8.2011.

[42] K. H. H.M. and K. S. Reddy, "DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network," *ACM Transactions on Internet Technology* , May 2025, doi: 10.1145/3737875.

[43] M. Soltani, K. Khajavi, M. J. Siavoshani, and A. H. Jahangir, "A multi-agent adaptive deep learning framework for online intrusion detection," *Cybersecurity* , vol. 7, no. 1, May 2024, doi: 10.1186/s42400-023-00199-0.

[44] J. Payne and A. Kundu, "Towards Deep Federated Defenses Against Malware in Cloud Ecosystems," p. 92, Dec. 2019, doi: 10.1109/tps-isa48467.2019.00020.

[45] A. Patel, D. S. Tomar, R. K. Pateriya, and R. Haripriya, "FL-MalDrift: a federated learning framework for malware detection under local concept drift," *Scientific Reports* , vol. 16, no. 1, p. 1821, Dec. 2025, doi: 10.1038/s41598-025-31592-z.

[46] A. Augello, A. D. Paola, and G. L. Re, "M2FD: Mobile malware federated detection under concept drift," *Computers & Security* , vol. 152, p. 104361, Feb. 2025, doi: 10.1016/j.cose.2025.104361.

[47] R. Gálvez, V. Moonsamy, and C. Díaz, "Less is More: A privacy-respecting Android malware classifier using federated learning," *Proceedings on Privacy Enhancing Technologies* , vol. 2021, no. 4, p. 96, Jul. 2021, doi: 10.2478/popets-2021-0062.

[48] F. Nawshin, R. Gad, D. Ünal, A. Al-Ali, and P. N. Suganthan, "Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey," *Computers & Electrical Engineering* , vol. 117, p. 109233, Apr. 2024, doi: 10.1016/j.compeleceng.2024.109233.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[49] F. Ceschin, M. Botacin, H. M. Gomes, F. Pinagé, L. S. Oliveira, and A. Grégio, "Fast & Furious: On the modelling of malware detection as an evolving data stream," *Expert Systems with Applications* , vol. 212, p. 118590, Aug. 2022, doi: 10.1016/j.eswa.2022.118590.

[50] F. Ceschin, M. Botacin, H. M. Gomes, F. Pinagé, L. S. de Oliveira, and A. Grégio, "Fast & Furious: Modelling Malware Detection as Evolving Data Streams," *arXiv (Cornell University)* , May 2022, Accessed: Oct. 2025. [Online]. Available: http://arxiv.org/abs/2205.12311

[51] A. Herzog, A. Eusebi, and L. Cavallaro, "On the Reliability and Stability of Selective Methods in Malware Classification Tasks," *arXiv (Cornell University)* , May 2025, doi: 10.48550/arxiv.2505.22843.

[52] R. Kapoor, J. Joshua, M. Vijayarangan, and B. Natarajan, "FedCL-Ensemble Learning: A Framework of Federated Continual Learning with Ensemble Transfer Learning Enhanced for Alzheimer's MRI Classifications while Preserving Privacy," *arXiv (Cornell University)* , Nov. 2024, doi: 10.48550/arxiv.2411.12756.

[53] V. Lakshmi and R. Sujatha, "Hybrid Ensemble Federated Learning Using Smote-Tomek for Efficient Ddos Detection on Constrained Edge Devices Over 5g Networks," *SSRN Electronic Journal* , Jan. 2025, doi: 10.2139/ssrn.5348369.

[54] F. E. Casado, D. Lema, R. Iglesias, C. V. Regueiro, and S. Barro, "Ensemble and continual federated learning for classification tasks," *Machine Learning* , vol. 112, no. 9, p. 3413, May 2023, doi: 10.1007/s10994-023-06330-z.

[55] Y. Bi, Y. Li, X. Feng, and X. Mi, "Enabling Privacy-Preserving Cyber Threat Detection with Federated Learning," *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.05130.

[56] Md. M. Abedin and T. Mehrub, "Evaluating Ensemble and Deep Learning Models for Static Malware Detection with Dimensionality Reduction Using the EMBER Dataset," *arXiv (Cornell University)* , Jul. 2025, doi: 10.48550/arxiv.2507.16952.

[57] M. Rahmati, "Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.10599.

[58] A. Guerra-Manzanares, M. Luckner, and H. Bahşi, "Concept drift and cross-device behavior: Challenges and implications for effective android malware detection," *Computers & Security* , vol. 120, p. 102757, May 2022, doi: 10.1016/j.cose.2022.102757.

[59] T. T. Chow, Z. Kan, L. Linhardt, L. Cavallaro, D. J. Arp, and F. Pierazzi, "Drift Forensics of Malware Classifiers," p. 197, Nov. 2023, doi: 10.1145/3605764.3623918.

[60] B. Molina-Coronado, U. Mori, A. Mendiburu, and J. Miguel-Alonso, "Efficient Concept Drift Handling for Batch Android Malware Detection Models," *arXiv (Cornell University)* , Sep. 2023, doi: 10.48550/arxiv.2309.09807.

[61] A. Davarasan, J. Samual, K. Palansundram, and A. Ali, "A Comprehensive Review of Machine Learning Approaches for Android Malware Detection," *Journal of Cyber Security and Risk Auditing* , vol. 2024, no. 1. p. 39, Dec. 06, 2024. doi: 10.63180/jcsra.thestap.2024.1.5.

[62] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Frontiers in Big Data* , vol. 7, p. 1497535, Dec. 2024, doi: 10.3389/fdata.2024.1497535.

[63] D. M. Trung *et al.* , "DMLDroid: Deep Multimodal Fusion Framework for Android Malware Detection with Resilience to Code Obfuscation and Adversarial Perturbations," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.11187.

[64] Y. Liu, C. Tantithamthavorn, L. Li, and Y. Liu, "Deep Learning for Android Malware Defenses: A Systematic Literature Review," *ACM Computing Surveys* , vol. 55, no. 8. Association for Computing Machinery, p. 1, Jun. 22, 2022. doi: 10.1145/3544968.

[65] Y. Chen, Z. Ding, and D. Wagner, "Continuous Learning for Android Malware Detection," *arXiv (Cornell University)* , Feb. 2023, doi: 10.48550/arxiv.2302.04332.

[66] A. Sabbah, R. Jarrar, S. Zein, and D. Mohaisen, "Empirical Evaluation of Concept Drift in ML-Based Android Malware Detection," 2025, doi: 10.48550/ARXIV.2507.22772.

[67] M. Chaieb, M. A. Ghorab, and M. A. Saied, "Detecting Android Malware: From Neural Embeddings to Hands-On Validation with BERTroid," *arXiv (Cornell University)* , May 2024, doi: 10.48550/arxiv.2405.03620.

[68] SK. H. Kauser and V. M. Anu, "Hybrid deep learning model for accurate and efficient android malware detection using DBN-GRU," *PLoS ONE* , vol. 20, no. 5, May 2025, doi: 10.1371/journal.pone.0310230.

[69] N. I. Hasanah, G. P. Insany, I. L. Kharisma, and N. D. Rahayu, "Recent Advancements in Machine Learning Models for Malware Detection: A Systematic Literature Review," p. 78, Sep. 2025, doi: 10.3390/engproc2025107078.

[70] S. Berríos, D. Leiva, B. Olivares, H. Allende-Cid, and P. Hermosilla, "Systematic Review: Malware Detection and Classification in Cybersecurity," *Applied Sciences* , vol. 15, no. 14, p. 7747, Jul. 2025, doi: 10.3390/app15147747.

[71] B. P. Gond and D. P. Mohapatra, "Deep Learning-Driven Malware Classification with API Call Sequence Analysis and Concept Drift Handling," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.08679.

[72] S. Nazim, M. M. Alam, S. S. A. Rizvi, J. C. Mustapha, S. S. Hussain, and M. M. Su'ud, "Multimodal malware classification using proposed ensemble deep neural network framework," *Scientific Reports* , vol. 15, no. 1, p. 18006, May 2025, doi: 10.1038/s41598-025-96203-3.

[73] S. K. Dey, W. Sarma, and S. Tiwari, "Deep learning applications for real-time cybersecurity threat analysis in distributed cloud systems," *World Journal of Advanced Research and Reviews* , vol. 17, no. 3, p. 1044, Mar. 2023, doi: 10.30574/wjarr.2023.17.3.0288.

[74] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal Of Big Data* , vol. 11, no. 1. Springer Science+Business Media, Aug. 04, 2024. doi: 10.1186/s40537-024-00957-y.

[75] M. O. Okafor, "Deep learning in cybersecurity: Enhancing threat detection and response," *World Journal of Advanced Research and Reviews* , vol. 24, no. 3, p. 1116, Dec. 2024, doi: 10.30574/wjarr.2024.24.3.3819.

[76] "Security Paradigms for SDN-IoT Convergence: Integrating Agentic AI Agents, Blockchain, and Graph Neural Networks for Threat Resilience."

[77] J. P. Bharadiya, "Machine Learning in Cybersecurity: Techniques and Challenges," *European Journal of Technology* , vol. 7, no. 2, p. 1, Jun. 2023, doi: 10.47672/ejt.1486.

[78] D. O. Babalola *et al.* , "AI-Powered Cybersecurity in Edge Computing: Lightweight Neural Models for Anomaly Detection," *International Journal of Multidisciplinary Research and Growth Evaluation* , vol. 5, no. 2, p. 1130, Jan. 2024, doi: 10.54660/.ijmrge.2024.5.2.1130-1138.

[79] A. Amandeep, "Cybersentinel AI: An Intelligent Cybersecurity Framework Using Artificial Intelligence," *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 6, p. 2679, Jun. 2025, doi: 10.22214/ijraset.2025.72761.

[80] S. S. Sefati, B. Arasteh, S. Halunga, and O. Fratu, "A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT)," *Cluster Computing* , vol. 28, no. 12, Sep. 2025, doi: 10.1007/s10586-025-05449-z.

[81] V. Pai, K. R. M. Pai, S. Manjunatha, S. Hirmeti, and V. Bhat, "Adaptive network anomaly detection using machine learning approaches," *EURASIP Journal on Information Security* , vol. 2025, no. 1, Oct. 2025, doi: 10.1186/s13635-025-00216-4.

[82] V. Chiniwar, "An Extensive Survey on Malware Detection and Prevention Mechanisms Using Advanced Technologies," *International Journal for Research in Applied Science and Engineering Technology* , vol. 13, no. 7, p. 2175, Jul. 2025, doi: 10.22214/ijraset.2025.73342.

[83] "Machine Learning and Deep Learning Approaches for Malicious Network Traffic Detection: A Comprehensive Evaluation."

[84] A. K. B. Arnob, R. R. Chowdhury, N. A. Chaiti, S. K. Saha, and A. N. U. Roy, "A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions," *Journal of Edge Computing* , vol. 4, no. 1, p. 73, Apr. 2025, doi: 10.55056/jec.885.

[85] J. Tian and H. Zhu, "Evaluating the efficacy of AI-driven intrusion detection systems in IoT: a review of performance metrics and cybersecurity

threats," *PeerJ Computer Science* , vol. 11, Nov. 2025, doi: 10.7717/peerj-cs.3352.

[86] A. K. A. Hwaitat *et al.* , "Overview of Mobile Attack Detection and Prevention Techniques Using Machine Learning," *International Journal of Interactive Mobile Technologies (iJIM)* , vol. 18, no. 10, p. 125, May 2024, doi: 10.3991/ijim.v18i10.46485.

[87] E. Rodríguez, B. Otero, N. Gutiérrez, and R. Canal, "A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks," *IEEE Communications Surveys & Tutorials* , vol. 23, no. 3, p. 1920, Jan. 2021, doi: 10.1109/comst.2021.3086296.

[88] M. M. Aslam, A. Tufail, H. Gul, M. N. Irshad, and A. Namoun, "Artificial intelligence for secure and sustainable industrial control systems - A Survey of challenges and solutions," *Artificial Intelligence Review* , vol. 58, no. 11, Aug. 2025, doi: 10.1007/s10462-025-11320-9.

[89] I. K. Nti, M. S. Manikanta, C. Alex, and N. Li, "Lightweight Neural Anomaly Detection for Resource-Constrained Edge-ICN Environments: A Systematic Literature Review," *Research Square (Research Square)* , Nov. 2025, doi: 10.21203/rs.3.rs-8002082/v1.

[90] M. Y. Saeed *et al.* , "Collaborative multi-agent XRL for threat detection in mobile edge network traffic," *Complex & Intelligent Systems* , vol. 11, no. 10, Sep. 2025, doi: 10.1007/s40747-025-02079-1.

[91] S. F. Misrak and H. M. Melaku, "Lightweight intrusion detection system for IoT with improved feature engineering and advanced dynamic quantization," *Discover Internet of Things* , vol. 5, no. 1, Sep. 2025, doi: 10.1007/s43926-025-00203-8.

[92] U. Abiha *et al.* , "Improving adversarial resilience for anomaly detection in the heterogeneous internet of things through ensemble models," *Future Generation Computer Systems* , vol. 178, p. 108299, Dec. 2025, doi: 10.1016/j.future.2025.108299.

[93] M. Ramaiah, V. Chandrasekaran, P. Adla, A. Vasudevan, M. F. A. Hunitie, and S. I. S. Mohammad, "Optimal feature selection based on OCS for improved malware detection in IoT networks using an ensemble classifier," *International Journal of Data and Network Science* , vol. 8, no. 4, p. 2127, Jan. 2024, doi: 10.5267/j.ijdns.2024.6.018.

[94] H. M. Al, M. S. Alm, and K. Dr, "Detecting malicious traffic in the network packets based on machine learning and deep learning approaches."

[95] S. Euh, H. Lee, D. Kim, and D. Hwang, "Comparative Analysis of Low-Dimensional Features and Tree-Based Ensembles for Malware Detection Systems," *IEEE Access* , vol. 8, p. 76796, Jan. 2020, doi: 10.1109/access.2020.2986014.

[96] I. M. Ibrahim and A. B. Sallow, "Feature Selection for Android Malware Detection with Random Forest on Smartphones," *Revue d intelligence artificielle* , vol. 37, no. 4, p. 857, Aug. 2023, doi: 10.18280/ria.370405.

[97] F. S. Alsubaei, A. A. Almazroi, W. Atwa, A. A. Almazroi, N. Ayub, and N. Z. Jhanjhi, "BERT ensemble based MBR framework for android malware detection," *Scientific Reports* , vol. 15, no. 1, p. 14027, Apr. 2025, doi: 10.1038/s41598-025-98596-7.

[98] M. M. Abualhaj *et al.* , "A bio inspired hybrid optimization framework for efficient real time malware detection," *Scientific Reports* , vol. 16, no. 1, p. 4542, Jan. 2026, doi: 10.1038/s41598-025-33439

[99] R. Alghamdi and M. Bellaïche, "An ensemble deep learning based IDS for IoT using Lambda architecture," *Cybersecurity* , vol. 6, no. 1, Mar. 2023, doi: 10.1186/s42400-022-00133-w.

[100] N. Ibrahim and N. R. Rajalakshmi, "Examining the Influence of Advanced Persistent Threats on Higher Education Institutions and Investigating Appropriate Cybersecurity Strategies," *U Porto Journal of Engineering* , vol. 11, no. 2, p. 96, Oct. 2025, doi: 10.24840/2183-6493_0011-002_002671.

[101] L. Yao, Q. Shi, Z. Yang, S. Shao, and S. Hariri, "Development of an Edge Resilient ML Ensemble to Tolerate ICS Adversarial Attacks," *arXiv (Cornell University)* , Sep. 2024, doi: 10.48550/arxiv.2409.18244.

[102] S. P. Praveen, K. Sharma, D. Parashar, V. S. N. Murthy, U. Sirisha, and D. A. Dewi, "Design of an iterative method for adaptive federated intrusion detection for energy-constrained edge-centric 6G IoT cyber-physical systems," *Scientific Reports* , vol. 15, no. 1, p. 41387, Nov. 2025, doi: 10.1038/s41598-025-25293-w.

[103] L. P. Byrapuneni and M. Saidireddy, "An Efficient Cluster Based Multi-Label Classification Model for Advanced Persistent Threat Attacks Detecting," *International Journal of Safety and Security Engineering* , vol. 14, no. 2, p. 541, Apr. 2024, doi: 10.18280/ijsse.140221.

[104] T. Hasan, A. Hossain, M. A. Ansari, and T. Syed, "Enhanced Intrusion Detection in IIoT Networks: A Lightweight Approach with Autoencoder-Based Feature Learning," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.15266.

[105] J. Wang *et al.* , "Self-learning model fusion for network anomaly detection: A hybrid CNN-LSTM-transformer framework," *PLoS ONE* , vol. 20, no. 10, Oct. 2025, doi: 10.1371/journal.pone.0332502.

[106] N. Ibrahim, N. R. Rajalakshmi, V. Sivakumar, and L. Sharmila, "An optimized hybrid ensemble machine learning model combining multiple classifiers for detecting advanced persistent threats in networks," *Journal Of Big Data* , vol. 12, no. 1, Aug. 2025, doi: 10.1186/s40537-025-01272-w.

[107] L. Yang and A. Shami, "Toward Autonomous and Efficient Cybersecurity: A Multi-Objective AutoML-Based Intrusion Detection System," *IEEE Transactions on Machine Learning in Communications and Networking* , vol. 3, p. 1244, Jan. 2025, doi: 10.1109/tmlcn.2025.3631379.

[108] S. H. Almotiri, "AI driven IOMT security framework for advanced malware and ransomware detection in SDN," *Journal of Cloud Computing Advances Systems and Applications* , vol. 14, no. 1, Apr. 2025, doi: 10.1186/s13677-025-00745-w.

[109] V. Jyothsna, K. P. Dasari, S. Inuguru, V. B. R. Gowni, J. T. R. Kudumula, and K. Srilakshmi, "Unified Approach for Android Malware Detection: Feature Combination and Ensemble Classifier," in *Advances in computer science research* , Atlantis Press, 2024, p. 485. doi: 10.2991/978-94-6463-471-6_47.

[110] M. E. Eren *et al.* , "Catch'em all: Classification of Rare, Prominent, and Novel Malware Families," *arXiv (Cornell University)* , Mar. 2024, doi: 10.48550/arxiv.2403.02546.

[111] M. Adil, M. A. Jan, S. B. Hakim, H. Song, and Z. Jin, "xIDS-EnsembleGuard: An Explainable Ensemble Learning-based Intrusion Detection System," *arXiv (Cornell University)* , Mar. 2025, doi: 10.48550/arxiv.2503.00615.

[112] N. Cassavia, L. Caviglione, M. Guarascio, A. Liguori, and M. Zuppelli, "Learning autoencoder ensembles for detecting malware hidden communications in IoT ecosystems," *Journal of Intelligent Information Systems* , vol. 62, no. 4, p. 925, Nov. 2023, doi: 10.1007/s10844-023-00819-8.

[113] I. Bibers, O. Arreche, and M. Abdallah, "A Comprehensive Comparative Study of Individual ML Models and Ensemble Strategies for Network Intrusion Detection Systems," *arXiv (Cornell University)* , Oct. 2024, doi: 10.48550/arxiv.2410.15597.

[114] T. Yang and J. Sun, "A hybrid ensemble deep learning framework with novel metaheuristic optimization for scalable malicious website detection," *Scientific Reports* , vol. 15, no. 1, p. 44630, Dec. 2025, doi: 10.1038/s41598-025-33695-z.

[115] S. N. Zeleke, A. F. Jember, and M. Bochicchio, "Integrating Explainable AI for Effective Malware Detection in Encrypted Network Traffic." Jan. 09, 2025.

[116] N. Niknami, V. Mahzoon, S. Vučetić, and J. Wu, "Enhanced Meta-IDS: Adaptive multi-stage IDS with sequential model adjustments," *High-Confidence Computing* , vol. 5, no. 3, p. 100298, Jan. 2025, doi: 10.1016/j.hcc.2025.100298.

[117] I. Mutambik, "AI-Driven Cybersecurity in IoT: Adaptive Malware Detection and Lightweight Encryption via TRIM-SEC Framework," *Sensors* , vol. 25, no. 22, p. 7072, Nov. 2025, doi: 10.3390/s25227072.

[118] G. K. S. Kumar, K. Prakash, B. Muniyal, and M. Rajarajan, "Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles Against Advanced Persistent Threats," *IEEE Open Journal of Vehicular Technology* , vol. 6, p. 1438, Jan. 2025, doi: 10.1109/ojvt.2025.3576366.

[119] A. Muzaffar, H. R. Hassen, H. Zantout, and M. A. Lones, "Reassessing feature-based Android malware detection in a contemporary context," *arXiv (Cornell University)* , Jan. 2023, doi: 10.48550/arxiv.2301.12778.

[120] M. Chemmakha, O. Habibi, and M. Lazaar, "Improving Machine Learning Models for Malware Detection Using Embedded Feature Selection

Method," *IFAC-PapersOnLine* , vol. 55, no. 12, p. 771, Jan. 2022, doi: 10.1016/j.ifacol.2022.07.406.

[121] N. Khan, A. Al-Tamimi, A. Bermak, and I. Khalil, "Adaptive Malware Detection using Sequential Feature Selection: A Dueling Double Deep Q-Network (D3QN) Framework for Intelligent Classification," *arXiv (Cornell University)* , Jul. 2025, doi: 10.48550/arxiv.2507.04372.

[122] S. Aurangzeb, M. Aleem, M. T. Khan, H. Anwar, and M. S. Siddique, "CyberSecurity for Autonomous Vehicles Against Malware Attacks in Smart-Cities," *Research Square (Research Square)* , Nov. 2022, doi: 10.21203/rs.3.rs-2295674/v1.

[123] H. Bostani, J. Cortellazzi, D. J. Arp, F. Pierazzi, V. Moonsamy, and L. Cavallaro, "On the Effectiveness of Adversarial Training on Malware Classifiers," *arXiv (Cornell University)* , Dec. 2024, doi: 10.48550/arxiv.2412.18218.

[124] M. K. Alzaylaee, F. Almarshad, G. A. Gashgari, D. Algawiaz, and A. I. A. Alzahrani, "Advancing cybersecurity: AI-driven computer vision and machine learning models for real-time threat detection and prevention," *Journal of Engineering Research* , Jan. 2026, doi: 10.1016/j.jer.2026.01.014.

[125] O. A. Madamidola, F. Ngobigha, and A. Ez-zizi, "Detecting new obfuscated malware variants: A lightweight and interpretable machine learning approach," *arXiv (Cornell University)* , Jul. 2024, doi: 10.48550/arxiv.2407.07918.

[126] M. A. Yagiz and P. Göktaş, "LENS-XAI: Redefining Lightweight and Explainable Network Security through Knowledge Distillation and Variational Autoencoders for Scalable Intrusion Detection in Cybersecurity," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.00790.

[127] C. Atheeq, R. Sultana, S. A. Sabahath, and M. A. K. Mohammed, "Advancing IoT Cybersecurity: Adaptive Threat Identification with Deep Learning in Cyber-Physical Systems," *Engineering Technology & Applied Science Research* , vol. 14, no. 2, p. 13559, Apr. 2024, doi: 10.48084/etasr.6969.

[128] A. M. Elshewey and A. M. Osman, "Enhancing encrypted HTTPS traffic classification based on stacked deep ensembles models," *Scientific Reports* , vol. 15, no. 1, Oct. 2025, doi: 10.1038/s41598-025-21261-6.

[129] M. Adil, M. A. Jan, S. B. Hakim, H. Song, and Z. Jin, "xIDS-EnsembleGuard: An Explainable Ensemble Learning-based Intrusion Detection System," p. 93, Dec. 2024, doi: 10.1109/trustcom63139.2024.00040.

[130] X. Feng *et al.* , "Time-Constrained Ensemble Sensing With Heterogeneous IoT Devices in Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems* , vol. 24, no. 11, p. 12949, May 2022, doi: 10.1109/tits.2022.3170028.

[131] M. Malka, E. Farhan, H. Morgenstern, and N. Shlezinger, "Decentralized Low-Latency Collaborative Inference via Ensembles on the Edge," *IEEE Transactions on Wireless Communications* , p. 1, Jan. 2024, doi: 10.1109/twc.2024.3497167.

[132] C.-G. Wang, Z. Ma, Q. Li, D. Zhao, and F. Wang, "A Lightweight IoT Malware Detection and Family Classification Method," *Journal of Computer and Communications* , vol. 12, no. 4, p. 201, Jan. 2024, doi: 10.4236/jcc.2024.124015.

[133] M. J. C. S. Reis, "Edge-FLGuard: A Federated Learning Framework for Real-Time Anomaly Detection in 5G-Enabled IoT Ecosystems," *Applied Sciences* , vol. 15, no. 12, p. 6452, Jun. 2025, doi: 10.3390/app15126452.

[134] C. Feng *et al.* , "CyberForce: A Federated Reinforcement Learning Framework for Malware Mitigation," *IEEE Transactions on Dependable and Secure Computing* , vol. 22, no. 4, p. 4398, Mar. 2025, doi: 10.1109/tdsc.2025.3547005.

[135] S. A. Steven and S.-S. Ho, "Federated Learning Based Autoencoder Ensemble System for Malware Detection on Internet of Things Devices," *SSRN Electronic Journal* , Jan. 2024, doi: 10.2139/ssrn.4884051.

[136] Y. Wang and X. Yang, "Design and implementation of a distributed security threat detection system integrating federated learning and multimodal LLM," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.17763.

[137] R. Ranpara, S. K. Patel, O. P. Kumar, and F. A. Al-Zahrani, "Scalable architecture for autonomous malware detection and defense in software-defined networks using federated learning approaches," *Scientific Reports* , vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-14512-z.

[138] F. Folino, G. Folino, F. S. Pisani, L. Pontieri, and P. Sabatino, "Efficiently approaching vertical federated learning by combining data reduction and conditional computation techniques," *Journal Of Big Data* , vol. 11, no. 1, May 2024, doi: 10.1186/s40537-024-00933-6.

[139] K. Billah ElMouatez and D. Mourad, "Resilient and Adaptive Framework for Large Scale Android Malware Fingerprinting using Deep Learning and NLP Techniques," *arXiv (Cornell University)* , Feb. 2022, doi: 10.48550/arxiv.2105.13491.

[140] R. Islam, M. I. Sayed, S. Saha, M. J. Hossain, and M. A. Masud, "Android malware classification using optimum feature selection and ensemble machine learning," *Internet of Things and Cyber-Physical Systems* , vol. 3, p. 100, Jan. 2023, doi: 10.1016/j.iotcps.2023.03.001.

[141] N. Blaas, J. Winterbourne, W. Beauregarde, and E. Heathcote, "Ransomware Detection Through Contextual Behavior Mapping and Sequential Dependency Analysis," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5527159/v1.

[142] L. Yang and A. Shami, "A Multi-Stage Automated Online Network Data Stream Analytics Framework for IIoT Systems," *IEEE Transactions on Industrial Informatics* , vol. 19, no. 2, p. 2107, Oct. 2022, doi: 10.1109/tii.2022.3212003.

[143] A. S. Narayanan, M. Chandramohan, L. Chen, and Y. Liu, "Context-aware, Adaptive and Scalable Android Malware Detection through Online Learning (extended version)," *arXiv (Cornell University)* , Mar. 2022, doi: 10.48550/arxiv.1706.00947.

[144] I. Kraidia, A. Ghenai, and S. B. Belhaouari, "Defense against adversarial attacks: robust and efficient compressed optimized neural networks," *Scientific Reports* , vol. 14, no. 1, Mar. 2024, doi: 10.1038/s41598-024-56259-z.

[145] R. Morganti, J. R. Thompson, S. Jackson, D. A. Roberts, and N. Anderson, "Modern Ransomware Detection Using Adaptive Flexible Temporal Feature Integration," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5400328/v1.

[146] D. Friehauf, A. King, B. Oakley, R. Wright, and D. Caraway, "Adaptive Graph-Based Neural Signatures for Autonomous Ransomware Detection," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5468445/v1.

[147] M. Eisa, Q. Yardley, R. Witherspoon, H. Pendlebury, and C. Rutherford, "Semantic Entanglement-Based Ransomware Detection via Probabilistic Latent Encryption Mapping," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.02730.

[148] P. Knaapen, H. Carter, C. Davies, G. Robinson, and T. Martin, "A Novel Quantum-Backed Decision Vector Framework for Ransomware Detection Using Nonlinear Signal Entropy Mapping," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5497437/v1.

[149] D. Ayanara, A. Hillingworth, J. Casselbury, and D. Montague, "Spectral Entanglement Fingerprinting: A Novel Framework for Ransomware Detection Using Cross-Frequency Anomalous Waveform Signatures," *arXiv (Cornell University)* , Feb. 2025, doi: 10.48550/arxiv.2502.01275.

[150] K. M. Shafin, G. M. A. A. Kafi, and S. Reno, "Guardians of the Network: An Ensemble Learning Framework With Adversarial Alignment for Evasive Cyber Threat Detection," *Engineering Reports* , vol. 7, no. 10, Sep. 2025, doi: 10.1002/eng2.70419.

[151] M. Snave, R. Klein, M. Hayes, S. S. Nielsen, and T. Blanchard, "Classification of Ransomware Variants Through Adaptive Pattern Recognition in Real-Time Environments," *Research Square (Research Square)* , Nov. 2024, doi: 10.21203/rs.3.rs-5398213/v1.

[152] A. Hocosaj, C. Pendleton, and J. Churchill. Stoddard, "Detection of Stealthy Encryption in Ransomware Using AI-Driven Anomaly Detection Models," *Research Square (Research Square)* , Aug. 2024, doi: 10.21203/rs.3.rs-4955370/v1.

[153] Z. Awad, M. Zakaria, and R. Hassan, "An enhanced ensemble defense framework for boosting adversarial robustness of intrusion detection systems," *Scientific Reports* , vol. 15, no. 1, p. 14177, Apr. 2025, doi: 10.1038/s41598-025-94023-z.

[154] A. Aldaej, I. Ullah, T. A. Ahanger, and M. Atiquzzaman, "Ensemble technique of intrusion detection for IoT-edge platform,"

Scientific Reports , vol. 14, no. 1, May 2024, doi: 10.1038/s41598-024-62435-y.

[155] S. Kanthimathi, S. Venkatraman, K. Jayasankar, P. J. T, and R. Jashwanth, "A Novel Self-Attention-Enabled Weighted Ensemble-Based Convolutional Neural Network Framework for Distributed Denial of Service Attack Classification," *arXiv (Cornell University)* , Sep. 2024, doi: 10.48550/arxiv.2409.00810.

[156] S. Chattopadhyay, A. K. Sahoo, and S. Jasola, "An Enhanced DDoS Attack Detection in Software-Defined-Networks using Ensemble Learning," *SN Computer Science* , vol. 5, no. 5, May 2024, doi: 10.1007/s42979-024-02938-7.

[157] S. A. Chelloug, "A Robust Approach for Multi Classification-Based Intrusion Detection through Stacking Deep Learning Models," *Computers, materials & continua/Computers, materials & continua (Print)* , vol. 79, no. 3, p. 4845, Jan. 2024, doi: 10.32604/cmc.2024.051539.

[158] M. Alsuwaiket, "ZeroDay-LLM: A Large Language Model Framework for Zero-Day Threat Detection in Cybersecurity," *Information* , vol. 16, no. 11, p. 939, Oct. 2025, doi: 10.3390/info16110939.

[159] S. Kasarapu, S. Shukla, and S. M. P. Dinakarrao, "Optimizing Malware Detection in IoT Networks: Leveraging Resource-Aware Distributed Computing for Enhanced Security," *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.10012.

[160] S. Kasarapu, S. Shukla, and S. M. P. Dinakarrao, "Enhancing IoT Malware Detection through Adaptive Model Parallelism and Resource Optimization," *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.08808.

[161] M. A. Aleisa, "Enhancing Security in CPS Industry 5.0 using Lightweight MobileNetV3 with Adaptive Optimization Technique," *Scientific Reports* , vol. 15, no. 1, p. 18677, May 2025, doi: 10.1038/s41598-025-00496-3.

[162] M. R. A. Khan, A. Y. Barnawi, A. Munir, Z. Alsalman, and D. M. S. Sanunga, "Lightweight Quantized XGBoost for Botnet Detection in Resource-Constrained IoT Networks," *IoT* , vol. 6, no. 4, p. 70, Nov. 2025, doi: 10.3390/iot6040070.

[163] S. Almansour, K. T. P. Yadav, L. M. Alkwai, N. S. Alghamdi, W. Viriyasitavat, and G. Dhiman, "Adaptive personalized federated learning with lightweight depthwise convolutional bottleneck network for novel intrusion detection system in internet of vehicles," *Scientific Reports* , vol. 15, no. 1, p. 35604, Oct. 2025, doi: 10.1038/s41598-025-17699-3.

[164] A. Alshamrani, "Federated hierarchical MARL for zero-shot cyber defense," *PLoS ONE* , vol. 20, no. 8, Aug. 2025, doi: 10.1371/journal.pone.0329969.

[165] S. Kumar, S. Indu, and G. S. Walia, "Optimal Unification of Static and Dynamic Features for Smartphone Security Analysis," *Intelligent Automation & Soft Computing* , vol. 35, no. 1, p. 1035, Jun. 2022, doi: 10.32604/iasc.2023.024469.

[166] M. Althunayyan, A. Javed, and O. Rana, "A robust multi-stage intrusion detection system for in-vehicle network security using hierarchical federated learning," *Vehicular Communications* , vol. 49, p. 100837, Aug. 2024, doi: 10.1016/j.vehcom.2024.100837.

[167] M. Chiranjeevi and A. Chavan, "Adversarial Error Mitigation Technique for Sensor Fusion Framework on Dynamic Edge Computing Platform," *Arabian Journal for Science and Engineering* , Oct. 2025, doi: 10.1007/s13369-025-10671-3.

[168] S. Rosyada, F. A. Rafrastara, A. M. P. Ramadhani, W. Ghozi, and W. Yassin, "Enhancing XGBoost Performance in Malware Detection through Chi-Squared Feature Selection," *Jurnal Sisfokom (Sistem Informasi dan Komputer)* , vol. 13, no. 3, p. 396, Nov. 2024, doi: 10.32736/sisfokom.v13i3.2293.

1109/tits.2025.3525505.

[169] B. Ajayi, B. Barakat, and K. McGarry, "Leveraging VAE-Derived Latent Spaces for Enhanced Malware Detection with Machine Learning Classifiers," *arXiv (Cornell University)* , Mar. 2025, doi: 10.48550/arxiv.2503.20803.

[170] A. A. Almazroi and N. Ayub, "Deep learning hybridization for improved malware detection in smart Internet of Things," *Scientific Reports* , vol. 14, no. 1, Apr. 2024, doi: 10.1038/s41598-024-57864

[171] A. Daulay, K. Ramli, D. Sudiana, R. Harwahyu, T. Hidayat, and N. R. Fachrurrozi, "A Novel Hybrid Model for High-Accuracy Malware Detection in The Internet of Medical Things (IoMT) Environment.," *IIUM Engineering Journal* , vol. 26, no. 3, p. 304, Sep. 2025, doi: 10.31436/iiumej.v26i3.3746.

[172] H. Khazane, M. Ridouani, F. Salahdine, and N. Kaabouch, "IoT Network Security based on Intrusion Detection System using Stacked Ensemble," *WSEAS TRANSACTIONS ON INFORMATION SCIENCE AND APPLICATIONS* , vol. 22, p. 466, Jun. 2025, doi: 10.37394/23209.2025.22.38.

[173] O. Mohamed, "Cross-Domain Malware Detection via Probability-Level Fusion of Lightweight Gradient Boosting Models," *arXiv (Cornell University)* , Aug. 2025, doi: 10.48550/arxiv.2509.00476.

[174] S. Ullah *et al.* , "Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets," *Scientific Reports* , vol. 15, no. 1, p. 31072, Aug. 2025, doi: 10.1038/s41598-025-16553-w.

[175] O. Güngör, I. R. Kale, J. Zhou, and T. Rosing, "LIGHT-HIDS: A Lightweight and Effective Machine Learning-Based Framework for Robust Host Intrusion Detection," *arXiv (Cornell University)* , Sep. 2025, doi: 10.48550/arxiv.2509.13464.

[176] P. Rani and K. Baalaji, "Deep learning-based ensemble stacking for enhanced intrusion detection in IoT-edge platforms," *Discover Applied Sciences* , vol. 7, no. 8, Aug. 2025, doi: 10.1007/s42452-025-06871-z.

[177] M. U. Tanveer, K. Munir, H. J. Alyamani, S. R. Hassan, M. Sheraz, and T. C. Chuah, "Graph-augmented multi-modal learning framework for robust android malware detection," *Scientific Reports* , vol. 15, no. 1, p. 38341, Nov. 2025, doi: 10.1038/s41598-025-22169-x.

[178] D. S, M. G. Shankar, E. Daniel, and B. G. Varghese, "Enhancing security in IoMT using federated TinyGAN for lightweight and accurate malware detection," *Scientific Reports* , vol. 16, no. 1, p. 7116, Feb. 2026, doi: 10.1038/s41598-026-37830-2.

[179] N. Dissanayake and U. Thayasivam, "Attack-Specialized Deep Learning with Ensemble Fusion for Network Anomaly Detection," *arXiv (Cornell University)* , Oct. 2025, doi: 10.48550/arxiv.2510.12455.

[180] G. Liu, D. Caragea, X. Ou, and S. Roy, "Benchmarking Android Malware Detection: Traditional vs. Deep Learning Models," 2025, doi: 10.48550/ARXIV.2502.15041.

[181] R. Darwish, M. Abdelsalam, and S. Khorsandroo, "Deep learning based XIoT malware analysis: A comprehensive survey, taxonomy, and research challenges," *Journal of Network and Computer Applications* , vol. 242, p. 104258, Jul. 2025, doi: 10.1016/j.jnca.2025.104258.

[182] R. Darwish, M. Abdelsalam, and S. Khorsandroo, "Deep Learning Based XIoT Malware Analysis: A Comprehensive Survey, Taxonomy, and Research Challenges," *arXiv (Cornell University)* , Oct. 2024, doi: 10.48550/arxiv.2410.13894.

[183] M. Wazid *et al.* , "Explainable Deep Learning-Enabled Malware Attack Detection for IoT-Enabled Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems* , vol. 26, no. 5, p. 7231, Jan. 2025, doi: 10.