IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

AI Based Malicious Activity Detection System

Prof. Anuja Phapale[1], Siddharth Mahore[2], Virendra Kharate[3], Pratik Karande[4], Viraj Kharat[5]
Professor, Department of Information Technology[1]
Student, Department of Information technology[2,3,4,5]
AISSMS Institute of Information Technology, Pune, Maharashtra, India

Abstract: *The increase in digital infrastructures in enterprise, mobile and cloud computing environments has resulted in a complex threat landscape making the use of older rule-based and signature-oriented security solutions insufficient. Network intrusion, malware infection, phishing attack, and even system level anomalies are forms of cyber threats that continue to exist, necessitating intelligent, adaptive and automated frameworks capable of identifying such threats. In this paper, a comprehensive overview and summary of AI and ML methods used in malicious activity detecting in four broad categories, namely, network intrusion detection, malware detection, phishing attack detection, and system-level anomalies, are presented. This paper is concentrated on the twenty peer-reviewed articles that have been published in the last two years and considers hybrid deep learning methods, behavioral analysis frameworks, NLP classification models, and ensemble learning. Among the key insights given, there are the higher performance of hybrid AI models over their counterparts in terms of recall, accuracy and false positive rate. These hybrid models, which integrate CNN, LSTM, GNN, and transformers have been discovered to be more effective in identifying cyber threats as compared to the individual models. This paper also highlights some of the difficulties associated with this technique such as unbalanced datasets, interpretability, adversarial robustness, computationally costly, and real-time constraints. A multi-level system of detection has been recommended where the network traffic is analyzed, endpoint behavior is monitored, communication is filtered with the help of natural language processing, and anomaly scoring is done by AI. These findings offer effective guidelines to practitioners and scholars on how to make future intelligent cyber defense systems able to be proactive in preventing threats*

Keywords: Machine Learning, Artificial Intelligence, Malicious Activity Detection, Network Intrusion Detection, Malware Detection, Phishing Detection, Anomaly Detection, Deep Learning, CNN, LSTM, GNN, Transformer, Cybersecurity, Behavioral Analysis, NLP

1. INTRODUCTION

The advent of technology to offer essential services such as banking, healthcare, commerce, education and governance has presented a vast threat arena to any evil being on a scale never experienced before. Cyber-attacks have now turned into more advanced tools of intrusion via automation, AI, and social engineering, by way of regular security protocols. The cost of cyber-crimes due to ransomware, data breaches, phishing, and Advanced Persistent Threats (APT) is expected to touch $10 trillion per year by 2025 [1].

Traditional security systems like antivirus engines based on signatures, rule-based firewalls, and static IDS relies on pattern recognition and prior knowledge. Despite being efficient when it comes to known and cataloged threats, conventional frameworks lack an inherent feature and are thus useless in three specific scenarios: first, when the threat is unknown such as in a zero-day attack; second, when the threat is polymorphic, such as some malware programs changing their signature every time they execute; third, when dealing with sophisticated phishing attacks mimicking natural conversations. There is an urgent requirement of smart structures, which are capable of learning in the process.

With the development of deep learning models, the emergence of Artificial Intelligence (AI) and Machine Learning (ML) has become a game-changer in cyber security. By training on very complex, multi-dimensional patterns in big

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 11, April 2026 Impact Factor: 8.2

data, AI has been in a position to be far more successful, identifying known and novel attacks with far fewer false alarms than the predecessors, which relied on rules. The examples of some of the most successful algorithms are CNN, LSTM networks, Graph Neural Networks (GNN), transformers, and GANs.

The presented paper includes the synthesis of findings of twenty scientific publications released in the last years in reputable journals in the field and concentrates on four main domains of threat detection methods using AI: (i) network intrusion detection; (ii) malware/ransomware detection; (iii) phishing/social engineering detection; and (iv) systems anomaly detection. The goal of this paper is to offer a systematic evaluation of the existing techniques, to highlight common trends, challenges, and opportunities, and to introduce an integrated multilayered detection approach.

Arrangement of the rest of the paper in the following way: The Literature Review will be discussed in section II with the main papers on each of the domains presented and a comparison table. In section III, the proposed System Architecture is discussed. Section IV presents results and a comparison of results. Conclusion and future directions are mentioned in section V.

II. LITERATURE REVIEW INTRODUCTION

A. Network Intrusion Detection Systems (NIDS)

One of the issues that have been addressed extensively in terms of AI in cybersecurity studies is the problem of network threat detection. Repalle and Kolluru (2017) established an important benchmark on the basis of classical supervised and unsupervised learning models KNN, SVM, Decision Trees, Naive Bayes, and K-Means which were applied to analyze the CTU-13 data set. KNN has been discovered to be the most suitable classifier and data quality to be the main predictor of the IDS performance [4]. Gopalsamy (2021) went further to demonstrate the strength of deep learning with CNN, LSTM, and ANN on the NSL-KDD data set as the CNN model of feature extraction had an accuracy and F1 score of 99.9% and 99%, respectively, because it was trained hierarchically.

Vijay et al. (2023) were the first to use biological optimization in deep learning as they implemented the BAT algorithm-based attention optimization into a Deep Convolutional Neural Network model with CICIDS2017 as its input benchmark. Although the overall accuracy levels were low (around 42%), the methodology never lost to SVM, Random Forest, and Naive Bayes algorithms in baseline testing, thus demonstrating the usefulness of bio-inspired mixed models in real-time network protection [6]. Park et al. (2023) have made the most influential innovation aimed at addressing the problem of the lack of data balance that is a frequent issue in NIDS research. They used Boundary Equilibrium Generative Adversarial Networks (BEGAN) to generate synthetic attack samples of minority classes and autoencoder-based feature analysis and deep learning (DNN), convolutional neural networks (CNN), and long-short-term-memory (LSTM) classifiers. In particular, G-CNNAE achieved a score of 93.2% in multi-classification on NSL-KDD and 93.8% in F1-score on the live data created at an enterprise Security Operation Centre within a period of five months [7].

B. Malware and Ransomware Detection

The detection of malware has become more dynamic and based on deep learning instead of comparing static signatures. Vinayakumar et al. (2019) introduced ScaleMalNet, a hybrid model that combines CNN, DNN, and LSTM to perform both static and dynamic malware analysis, which has demonstrated high detection accuracy compared to conventional methods and does not need manual feature engineering [1]. To overcome the particular issue of the fast evolution of ransomware, Khan et al. (2020) proposed a digital DNA sequencing framework that models application execution traces as structured behavioral sequences, which allows identifying never-seen variants by matching the pattern with existing behavioral profiles [2]. A broad survey by Aslan and Samet (2020) organized malware detection methods systematically in signature-based, anomaly-based, and ML-based paradigms, marking the imbalance of datasets, zero-day resistance, and complexity of feature selection as the most burning unresolved issues [3].

Altaha et al. (2024) tested supervised machine learning classifiers on Android malware with both static and dynamic features extraction and could demonstrate significant improvements over the current antivirus software programs based

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

on re-training as one of the necessary conditions of their implementation [14]. In the question of scalability of computation, Kim et al. (2024) suggested the application of Compact Data Learning (CDL) method that promotes the efficiency of training by reducing the quantity of the dataset, yet maintaining the predictiveness of the dataset, guaranteeing approximately 99 percent detection rate with different ML methods [15].

C. Phishing and Social Engineering Detection

Phishing attempts have become increasingly sophisticated due to the development of language models that are able to create convincing misleading content. Phishing in the form of emails or social networks have been surveyed in the literature on this topic. A study of NLP and ML using Logistic Regression and XGBoost on the linguistic features of AI phishing emails revealed that XGBoost achieves an accuracy rate of circa 98% and textual features like imperative verbs, personal pronouns and sentence construction still have a high discriminatory value when used on AI-generated texts [16]. PhishGuard-AI was an original contribution to this space that suggested a two-channel model that simultaneously processes semantic embeddings (BERT, RoBERTa) and stylistic measures (perplexity, lexical diversity, sentence rhythm), whereas the fusion layer allows it to outperform all single-channel models using hybrid transformers [17].

The multi-layered phishing-detection system based on SVM and deep neural networks proved to be efficient on an enterprise level in terms of analyzing the emails headers, URLs, content and attachments and could reduce the phishing attacks, however, it also experienced problems with adversarial robustness and Explainable AI [18]. Systematic review of the current methods of OSN spam and phishing detection and comparison of various methods based on URL, content, account and hybrid were carried out. It was identified that hybrid models based on the use of both NLP and data mining were the most suitable to deal with the OSN data because it is complex and noisy [19]. The research carried out by practitioners [20] generated best practices of applying AI algorithms to phishing detection.

D. System-Level and Behavioral Anomaly Detection

System level and behavioral anomaly detection strategies target very complex and context-sensitive attacks, which cannot be detected using network traffic or signature analysis methods. Mah et al. (2025) created an algorithm named Isolation Forest Algorithm Trees (IFAT) that is applicable in e-commerce to classify using interpretable decision trees with twelve attributes augmented by BERT and scores 0.83 in complaints, escalations, and refunds classification [9]. Conversely, with reference to enterprise security, Nwoye and Nwagwughiagwu (2024) have compared the results of SVM, Decision Trees, and Neural Network models on the KDD99/NSL-KDD data with data breach predictions and found out that the best results are achieved by the neural networks due to their overall accuracy (94%), precision (91%), and recall They also indicated that SHAP and LIME can be used to conduct XAI [10].

The appropriate analytical framework in the literature review given is the analysis by Aljumaily et al. (2025) in which the authors created an AI-enhanced UEBA model that incorporates LSTM Autoencoders, LogBERT transformers, and Graph Neural Networks (GNNs). When the researchers tested this combination on the CERT Insider Threat, UNSW-NB15, and TON_IoT datasets together with the use of Apache Kafka, their model that consists of Transformers and GNNs achieved an outstanding 0.93 F1 score, reduced false positives by 40%, and minimized incident triaging time from 18 minutes to 4 minutes, which means 78% efficiency compared to the traditional rule-based SIEM solutions [12]. Comparative analysis of the performance of the different algorithms, including Random Forest, DNN, SVM, KNN, and Logistic Regression, on the CICIoT2023 dataset, where SMOTE was used, showed that the Random Forest had 99.55% F1 score; however, the algorithm had a low 83.15% F1 score when addressing 34-class attacks [13].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

E. Comparative Literature Summary Table

Table 1: Major Literature Review Summary

Sr.	Authors & Year	Title	Domain	Methodology	Key Contribution	Limitations
1	Vinayakumar et al. (2019)	Robust Intelligent Malware Detection Using Deep Learning	Malware Detection	Hybrid CNN + DNN + LSTM, static + dynamic analysis	ScaleMalNet system; more accurate than signature-based methods	Expensive to compute; small number of diverse datasets
2	Khan et al. (2020)	Digital DNA Sequencing Engine for Ransomware Detection	Ransomware Detection	Digital DNA sequencing; machine learning behavioral fingerprinting	In real-time detection of ransomware; better classification accuracy	Fails against heavily obfuscated malware; requires constant updating
3	Aslan & Samet (2020)	A Comprehensive Review on Malware Detection Techniques	Malware Detection Survey	Systematic literature review; comparison of techniques	Classification of malware detection techniques; research gaps	Literature-based review without any empirical verification
4	Repalle & Kolluru (2017)	IDS Utilising AI & ML Algorithms	Network Intrusion	KNN, SVM, Decision Tree, Naïve Bayes on CTU-13	KNN most effective; uses active learning approach	Dataset important; unsupervised algorithms require manual adjustment
5	Gopalsamy (2021)	Advances in Cybersecurity through AI-Based NIDS	Network Intrusion	CNN, LSTM, ANN on NSL-KDD dataset; min-max scaling	CNN: 99.9% accuracy, 99% F1 score	Limited to NSL-KDD data; may not represent current traffic
6	Vijay, Sharma & Khanna (2023)	Transforming Network Operations with AI-Enabled IDS	Network Intrusion	BAT optimization & Deep CNN (BATO-DCNN); CICIDS2017	BATO-DCNN outperforms SVM, Random Forest, and Naïve Bayes	Moderate performance
7	Park et al. (2023)	Improved AI-Driven Network Intrusion Detection	Network Intrusion	BEGAN GAN, Autoencoder & Neural Networks	Accurately detects anomalies (93.2%) by addressing the class imbalance	Extremely unstable training process; need for adversarial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

Sr.	Authors & Year	Title	Domain	Methodology	Key Contribution	Limitations
		System Using GANs		(DNN, CNN or LSTM); Datasets (NSL-KDD, UNSW-NB15)	problem	robustness
8	Goswami (2024)	Improving Networking Security Using AI-Driven IDS	Network Intrusion	Ensemble learning techniques; streaming architectures; anomaly detection	Real time detection; low false alarms	Difficult to ensure privacy; computationally expensive; interpretable models not easy
9	Mah, Skalna & Pelech-Pilichowski (2025)	AI-Based Anomaly Detection in E-commerce Services	Anomaly / E-Commerce	IFAT + BERT-based NLP + Deep Learning Autoencoder	Tree-based QoS oriented anomaly detection; 0.83 accuracy	Small dataset (93 records); artificial biosignal data
10	Nwoye & Nwagwughiagwu (2024)	AI-Based Anomaly Detection to Enhance Cybersecurity	Cybersecurity / NIDS	Support Vector Machine, Decision Tree, Neural Network KDD99/NSL-KDD	Detector based on neural network: 94%, 91%, 90% for accuracy, precision, recall, respectively	Aged benchmarking datasets; black-box models
11	Ashish Kumar (2025)	Automated Usage Pattern Analyzer with the Help of AI	Telecom / IoT Anomaly	Review: Generative AI + Kafka + Distributed ML	Real-time fraud detection; mitigating alert fatigue	Only review; no empirical evidence; potential for model bias
12	Aljumaily, Abd & Majeed (2025)	Enhancing UEBA in SIEM Systems Using AI	Enterprise Security	LSTM Autoencoder + LogBERT + GNN on CERT/UNSW-NB15/TON_IoT	F1=0.93; 40% fewer false positives; 78% faster triage	GNN generalisation drops cross-domain; heavy inference cost
13	Akinade (2024)	AI-Driven Anomaly Detection for Cybersecurity in Healthcare	Healthcare / IoT	RF, DNN, SVM, KNN, LR on CICIoT2023; SMOTE balancing	RF: 99.55% binary F1; feature importance analysis	Single dataset; decreasing accuracy for 34-class scenario

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

Sr.	Authors & Year	Title	Domain	Methodology	Key Contribution	Limitations
14	Altaha et al. (2024)	Android Malware Detection Using Supervised ML	Mobile Security	Supervised ML classifiers; static + dynamic feature extraction	Improved detection accuracy for Android malicious apps	Privacy concerns; needs continuous retraining
15	Kim et al. (2024)	Malware Detection Using Advanced Machine Learning-Based Systems	Malware Detection	CDL using various machine learning models	Accuracy up to 99% with minimal dataset size	Tuning parameters and generalization issues
16	NLP/XGBoost Study (2023)	Social Engineering and Spam Detection in AI-Based Phishing Emails	Phishing / E-mail	Logistic regression, XGBoost, and linguistic feature analysis	XGBoost: nearly 98% accuracy, good interpretability	Depends on data sets; unable to process complicated texts
17	PhishGuard-AI (2024)	Phishing Detection 2.0: The NLP Solution for AI-Phishing	Phishing / Email	Dual-channel BERT and RoBERTa stylometry	Hybrid transformer performs better than individual models	Requires extensive computing power
18	Enterprise AI Study (2024)	AI-Based Phishing Detection in Organizations	Phishing / Organization	Multivariate analysis (email header, URL, body, attachment); SVM and DNN	Enhanced detection effectiveness and speed; practical examples	Data confidentiality; susceptibility to attacks; XAI required
19	OSN Survey (2023)	AI-driven Spam Filtering in Social Networking Sites	Phishing / Social Media	URL filtering, content filtering, account filtering + hybrid; NLP + DM	Taxonomy of OSN phishing; hybrid model approach	Noisy data; real-time challenges; dynamic nature of attacks
20	Best Practices Study (2024)	AI-Driven Phishing Detection - Challenges and Best Practices	Phishing / Policy	Machine Learning & NLP; behavioral and linguistic profiling; adaptive learning	Best practices for phishing detection using AI techniques	Dataset quality; adversarial attacks

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

III. SYSTEM ARCHITECTURE

Based on the literature review, a five-level architecture of AI-based malicious activity detection is proposed. All the tiers refer to a particular attack surface exposed in the domains that were identified in the literature review, hence a comprehensive solution to the enterprise security issues.

The architecture is implemented in a multi-layer security implementation whereby any threat that could not be stopped at the network frontier (Tier 1) will be intercepted either at the endpoint (Tier 2) or in the filtering of communications (Tier 3). The system anomaly detector (Tier 4) will identify behavior that has gone around all the earlier levels. Lastly, all alerts will be gathered and integrated in the SIEM integration level (Tier 5).

Table 2: Proposed System Architecture — Layer-by-Layer Description

Layer	Function	AI Techniques	Output
Layer 1: Network Traffic Monitor	Capture and classify incoming/outgoing packets	CNN, LSTM, GAN-augmented classifiers; NSL-KDD / CICIDS2017 trained	Intrusion alert with attack-type label
Layer 2: Endpoint Behavioral Engine	Monitor process, file, registry, and API call activity	ScaleMalNet (CNN+DNN+LSTM); Digital DNA sequencing; Random Forest	Malware classification (ransomware, trojan, zero-day)
Layer 3: Communication Screening	Scan emails, social messages, and URLs in real time	BERT / RoBERTa NLP; XGBoost; stylometric fusion (PhishGuard-AI)	Phishing / spam confidence score
Layer 4: System Anomaly Detector	Detect deviations in user/entity behavior and usage patterns	UEBA: LSTM Autoencoder + LogBERT + GNN; Isolation Forest	Anomaly score with SHAP explanation
Layer 5: SIEM Integration & Response	Correlate alerts, prioritize incidents, trigger playbooks	Transformer-GNN ensemble; role-aware prioritization	Ranked incident queue; automated response action

The following data flows through each layer: infrastructure layer gathers raw packets and system events and routes data stream to the respective processing pipelines using Apache Kafka. The alert signals are generated by each layer with confidence scores, and are forwarded to a SIEM integration layer even further. In Layer 4 and Layer 5, Graph Neural Networks are employed to identify connections between entities like users, hosts, processes to uncover the lateral movements and coordination of attacks that would be difficult to discover using a single layer. SHAP-based explanations are even incorporated in alerts, providing analysts with the tools they need to enhance the models through retraining.

The problem of class imbalance, which is equally prevalent in all domains addressed here, is addressed in the proposed system both through the use of GANs to generate synthetic data to be used in the training phases of Layers 1 and 4 and by use of SMOTE balancing of training data in Layers 2 and 3. The Layer 3 is proposed to be fedrated learning in the application with privacy relevance.

IV. RESULT

The overview of the metrics of the analyzed studies provides a number of trends that can be applied to the proposed architecture and detection of malicious activities through AI.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 11, April 2026 Impact Factor: 8.2

Deep learning models have a clear superiority over traditional machine learning counterparts in the network intrusion area in all metrics. Compared to the SVM (92) or the decision tree (89) by Nwoye and Nwagwughiagwu (2024), CNN models have achieved higher accuracy on the benchmarks, with 99.9% accuracy on NSL-KDD per Gopalsamy (2021). The fact that Park et al. (2023) have included data augmentation with the GAN methodology demonstrates that the issue of working with unbalanced datasets is just as important as the choice of the architecture, which G-CNNAE results in a higher recall of rare classes of attacks, growing by approximately 62 percent without data augmentation to 93.8 percent.

Hybrid models are more effective than single models in detecting malware. In ScaleMalNet, the combination of CNN, DNN, and LSTM algorithms will guarantee the complementary nature of the feature extraction features, i.e. CNN extracting spatial features of executable files, LSTM extracting temporal sequences, DNN allowing the interaction of the features, which cannot be attained using any single model architecture [1]. It can also be seen that based on the research conducted by Kim et al. (2024) on the optimization of CDL, it is possible to reach a similar accuracy rate (99%) with significantly smaller training sets [15].

In terms of accuracy, phishing detection is the best, as XGBoost reaches 98% with the help of solely linguistic features [16], while hybrid transformers obtain even greater accuracy from the fusion of stylometric features [17]. This is explained by the specifics of phishing attacks, the structure of which has a clear structure and needs a text-based analysis to be identified. PhishGuard-AI, which takes into consideration both semantic and stylistic attributes of text, is the most technologically advanced, particularly when it comes to machine learning-generated phishing attacks.

The Aljumaily et al. (2025) article about the application of the behavioral anomaly detection based on the UEBA paradigm offers the largest operational impact of the discussed works, as the time spent triaging incidents reduced by 78 percent, 18 minutes to less than 4 minutes [12]. This enhancement of the triaging is directly related to the MTTC which is a significant indicator of enterprise cybersecurity activities. Behavioral graph modeling with GNN shows particularly good results in the insider threat detection scenario, with an accuracy of 0.94 and an AUC-ROC of 0.96 on the CERT Insider Threat benchmark. However, domain generalizability remains an issue of GNN-based methods and precision declines between 0.94 and 0.84 when transferring between CERT and UNSW-NB15.

Regardless of all the above, there are three important observations that can be made which are typical of all the above areas. To start with, hybrid networks that involve the usage of more than one model are always superior to the usage of single models; the optimal model is the usage of LSTM (temporal), CNN (structural), and GNN (interaction) models. Second, interpretability with methods like SHAP, LIME, attention is not a nice-to-have but a necessary condition, as security staff members will not just act on the results produced by models that they do not understand. Lastly, class imbalances need to be corrected with the help of GANs, SMOTE, or CDL when the process of classification is not yet started.

V. CONCLUSION

In this research paper, the holistic application of AI and ML techniques in detecting malicious activities has been analyzed by reviewing twenty articles published in scholarly journals. It is found that AI-driven systems have shown qualitative superiority over conventional signature-based and rule-based approaches, and the integration of DL methods shows higher efficiency in all application domains.

Key findings of the research paper are as follows. First, deep neural network (CNN, LSTM, and GNN) methods show higher effectiveness than shallow methods in intrusion detection and malware detection because of their complexity, high-dimensional nature, and sequential properties. Second, NLP, transformer models like BERT and RoBERTa, and stylistic analysis methods have proven to be very effective for detecting phishing attacks that use AI-generated content. Third, behavioral analysis methods using UEBA, graph theory, and SIEM tools are more effective than other methods when it comes to efficiency. Generally, multimodal approaches outperform unimodal approaches, class balancing using GANs and SMOTE methods is critical for rare attack classification, and SHAP is vital for explainability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 11, April 2026 Impact Factor: 8.2

The proposed five-layered unified architecture in this paper integrates the most successful techniques from their individual domains to produce an efficient system for monitoring. Some directions worth exploring further in the domain of cyber security research are federated learning techniques to facilitate private distributed learning models, robustness analysis to ensure that models are robust against any targeted attacks, online learning techniques to handle emerging threats, and lightweight learning models on the edges in computing resource-constrained environments like IoT and mobile devices. The advancement of cyber security threats necessitates moving towards a fully adaptive model of cyber security.

REFERENCES

[1] Vinayakumar R et al. "Robust intelligent malware detection using deep learning," IEEE access, vol. 7, 2019. pp. 46717-46738. DOI: 10.1109/ACCESS.2019.2906934
[2] Khan ZA et al. "Digital DNA sequencing engine for ransomware detection using machine learning," IEEE access, vol. 8, 2020. pp. 119710-119726. DOI: 10.1109/ACCESS.2020.3003785
[3] Aslan O and Samet R. "A comprehensive review on malware detection approaches," IEEE access, vol. 8, 2020. pp. 6249-6271. DOI: 10.1109/ACCESS.2019.2963724
[4] S. A. Repalle and V. R. Kolluru, "An Intrusion Detection System using AI and Machine Learning Algorithms," IRJET, vol. 4, no. 12, pp. 1709-1715, Dec. 2017.
[5] M. Gopalsamy, "Advanced Cybersecurity for Network Intrusion Detection System based on AI Techniques," IJARSCT, vol. 5, no. 1, pp. 450-460, 2021.
[6] G. S. Vijay, M. Sharma, and R. Khanna, "Revolutionizing Network Management with an AI-Driven Intrusion Detection System," Multidisciplinary Science Journal, vol. 5, no. 3, 2023.
[7] C. Park et al., "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," IEEE IoT Journal, vol. 10, no. 3, pp. 2330-2345, Feb. 2023.
[8] M. J. Goswami, "Enhancing Networking Security with AI-Driven Intrusion Detection," IJOPE, vol. 12, no. 1, pp. 43-58, 2024.
[9] P. M. Mah, I. Skalna, and T. Pelech-Pilichowski, "AI-Driven Anomaly Detection in E-Commerce Services: NLP Approach to Isolation Forest Algorithm Trees," JTAECR (MDPI), vol. 20, no. 1, pp. 35-58, 2025.
[10] C. C. Nwoye and S. Nwagwughiagwu, "AI-Driven Anomaly Detection for Proactive Cybersecurity and Data Breach Prevention," IJETRM, vol. 8, no. 11, pp. 1-18, Nov. 2024.
[11] A. Kumar, "Automated Usage Pattern Analyzer: A Technical Review of Predictive Insights and Anomaly Detection Powered by AI," JCSTS, vol. 7, no. 3, pp. 98-118, Sep. 2025.
[12] M. S. Aljumaily, H. K. Abd, and E. J. Majeed, "Enhancing UEBA in SIEM Systems Using AI-Powered Anomaly Detection," IJMRAI, vol. 3, no. 4, pp. 77-103, Dec. 2025.
[13] S. K. Akinade, "Implementing AI-Driven Anomaly Detection for Cybersecurity in Healthcare Networks," JSTE ATBU, vol. 12, no. 2, pp. 211-238, Jun. 2024.
[14] M. Altaha et al., "A Survey on Android Malware Detection Techniques Using Supervised Machine Learning," IEEE Access, vol. 12, pp. 149870-149895, 2024. doi: 10.1109/ACCESS.2024.3485706
[15] J. Kim et al., "Advanced Machine Learning Based Malware Detection Systems," IEEE Access, vol. 12, pp. 112340-112358, 2024. doi: 10.1109/ACCESS.2024.3434629
[16] P. Anderson and K. Patel, "Social Engineering and Spam Detection of AI-Driven Phishing Emails," Proc. ISCA, pp. 214-221, 2023.
[17] L. Chen and Y. Wang, "Phishing Detection 2.0 - NLP Approach for AI-Generated Phishing," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 3401-3415, 2024.
[18] D. Martinez, F. Garcia, and M. Torres, "AI-Powered Phishing Detection in Enterprises," J. Netw. Comput. Appl., vol. 221, pp. 103789, Jan. 2024.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, April 2026
Impact Factor: 8.2

[19] R. Kumar and S. Sharma, "AI-Based Spam Detection Techniques for Online Social Networks," ACM Comput. Surv., vol. 55, no. 10, pp. 1-35, Oct. 2023.
[20] T. Williams and A. Johnson, "AI-Powered Phishing Detection - Challenges and Best Practices," IEEE Security Privacy, vol. 22, no. 1, pp. 45-58, Jan. 2024.