An AI-Based Intrusion Detection and Vulnerability Scanning Framework for Secure Networks

Prof. Rahul Pawar[1], Prof. Nilam Thorat[2], Disha Hublikar[3], Nikita Honrao[4], Mayuri Tapkire[5], Siddhi Shelke[6]
[1,2,3,4,5,6]*Vishwakarma Institute of Technology Pune, India*

***Abstract*—Due to the rapid rise of cybercrime and the increased complexity of network attacks, traditional Intrusion Detection Systems (IDS) are in most cases incapable of detecting sophisticated threats and zero-day vulnerabilities. To solve these problems, this article presents an AI-based Intrusion Detection and Vulnerability Scanning Framework that strengthens network defense with the help of intelligent automation. The system in question uses a Random Forest classifier trained on the widely-used NSL-KDD dataset to make accurate distinctions between malicious activity and normal traffic and thus, detection accuracy of 96.8% is achieved. Besides threat detection, there is also a real-time vulnerability scanner that identifies open ports, outdated or misconfigured services, and poses of known exploits before attackers target them. The experimental evaluation indicates that the proposed framework enhances precision and decreases the number of false alarms to a great extent if we compare it with traditional IDS models. In general, this paper is about a cybersecurity solution that is ahead of the curve and thus, organizations can detect, predict, and respond to new threats more efficiently in a continuously changing digital environment.**

***Index Terms*—Intrusion Detection System (IDS), Cybersecurity, Random Forest, Vulnerability Scanning, Network Security, Machine Learning**

I. INTRODUCTION

Intrusion Detection Systems (IDS) are security elements that track network or system operations. IDS habits aim to discover malicious behaviors or infringements of the policy. After all, they are the first to spot unauthorized access, strange traffic, or attempts to hack a company's network. Vulnerability scanning, by contrast, is a method where the majority of steps involved in locating security flaws, wrongly configured devices, and out-of-date software that hackers can exploit for illegal entry or disruption of the services are done automatically. Furthermore, these two security measures constitute the root of proactive cybersecurity when combined. Nevertheless, because of the rapid cyber threat evolution, traditional IDS and vulnerability scanners have hard times. Typical signature-based detection methods are limited to detecting only known patterns of attack and are incapable of finding zero-day attacks or even newly devised methods of intrusion that change continuously. Furthermore, these systems have an alarmingly high number of false positives. The number of false positives creates difficulties in prioritizing the real threats for administrators, thus making them unmanageable.

The use of Artificial Intelligence (AI) has been seen as a potent answer to circumvent the AI restrictions. To classify complex training examples in extensive data corpora and identify deviations from standards, AI methods such as machine learning and deep learning can be employed. In reality, these smart systems are always learning and changing as they are exposed to new situations; thus, they deliver better results and shorter response times. We present here an AI-driven intrusion detection and vulnerability scanning framework in this paper, which fuses intelligent anomaly detection with automated vulnerability assessment. The envisioned instrument is furtively data-driven with machine learning methods that detect intrusion complemented with a real-time scanning tool that helps in the identification of the breaking-in steps as well as system weak points. Through this combined strategy, the network defense is elevated because of the early detection, less false alarms, and full threat awareness.

II. LITERATURE SURVEY

Intrusion Detection Systems (IDS) are a must-have to pave the way for security and maintain the spoken-play of computer networks. Artificial Intelligence (AI) techniques are getting more attention from researchers in the last ten years among which Machine Learning (ML) and Deep Learning (DL) are the major ways to detect network anomalies and prevent cyberattacks. These AI-powered solutions work through the huge network traffic data, grasp the normal and attacked patterns, and find the differences that could signal an intrusion. But even with the advances in AI-based IDS, the current Lowell still can't solve problems of adaptability, scalability, and real-time response abilities.

The IEEE article named "Artificial Intelligence Based Intrusion Detection System a Detailed Survey" (Sharma et al., 2024) is a thorough overview of the present intrusion detection models and methods. It differentiates IDS into four categories namely supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning, each having its own strengths and weaknesses. Supervised learning methods such as Support Vector Machines (SVM), Decision Trees, and Random Forests are good performers when used with labelled datasets but can hardly manage skewed or unbalanced data distributions. Besides, they also need a lot of preprocessing and feature labelling that consumes a great deal of time. Unsupervised learning methods like K-means clustering are capable of discovering hidden patterns in data without assistance from labels but are often unable to provide precise classifications and are ill-equipped for handling real-time traffic. Semi-supervised learning uses a combination of labeled and unlabeled data to shorten the training time, however, if the ratio of unlabeled data is chosen incorrectly, the outcome could be a drop in performance. Reinforcement Learning (RL), which draws learning mechanisms from nature, could be the future of adaptive security applications. Unfortunately, it requires a large amount of computing resources and merges very slowly, especially in big-scale dynamic networks. The designed system layers four main units that work one after another and are each responsible for different security monitoring and analysis functions.

2.1 Data Collection Layer

The lowest level pulls together security-relevant data from several diverse sources to get full visibility over network infrastructure. This layer constantly keeps an eye on and collects network traffic patterns, system logs from all kinds of endpoints and servers, as well as vulnerability intelligence from well-maintained databases. By collecting data from multiple sources, the system ensures that no attacker can find a blind spot and that no vulnerability goes undiscovered, thus providing the raw material for the analysis stages that come next.

2.2 Preprocessing Layer

At the preprocessing layer, efforts are made to convert the raw data obtained into well-structured, machine-learning-friendly data forms. The data cleaning operations in this stage take care of removing noise, duplicates, and useless information, and at the same time, they deal with missing data. Feature extraction methods help to pinpoint and separate security-related features from the raw data streams that may be, for instance, packet headers, log patterns, or behavioral indicators. The normalization methods bring data to a standard form and adjust numerical values, thus supporting consistency across different data sources and making it possible for the computer to find patterns in the next steps.

2.3 Detection and Analysis Layer

The main brain layer is equipped with parallel processing units that can discover security threats through different but complementary methods. The AI-based Intrusion Detection System (IDS) module takes advantage of machine learning algorithms for the task of analyzing pre-processed network traffic and system behavior. Consequently, it can identify not only the attack signatures that it has already encountered but also the anomalous patterns that may lead to a discovery of new threats. In parallel, the Vulnerability Scan module checks out the system configurations, software versions, and security postures against a) database of known vulnerabilities, thus figuring out those weak points that have not been exploited yet. This dual-approach architecture facilitates not only the detection of threats that have been already triggered but also the management of vulnerabilities in a proactive way.

2.4 Response and Reporting Layer

The closing stage of the detection pipeline serves to turn the findings of the investigation into actions that can be taken by security operations through the use of both automated response mechanisms and detailed visualization. The security system makes records of the current situation in the network and reports on the threats and vulnerabilities that have been found, providing other details such as the degree of severity and possible impact. The automated response features provide the necessary support for defensive actions that can be carried out at once, thus ensuring the immediate reaction to the situation, as such activities may include, among others, traffic blocking, session termination, or system isolation, and should be carried out on the basis of the already established security policies. An incorporated dashboard offers security analysts easy-to-use visualization of the security posture, threat trends, and vulnerability status which is a great way for them to make informed decisions and coordinate their response to the incident.

The architecture that is both sequential and integrated nevertheless enables the organization of the data flow in a systematic manner while at the same time ensuring the modularity of the parts for the purposes of upgrading and customization. The parallel processing that takes place in the detection layer is one of the factors that result in the optimization of the computational resources as well as the reduction of the analysis time which is a step towards the detection of threats that are very close to the real-time ones. What is more, the integration of AI-based intrusion detection methods with the systematic vulnerability scanning techniques not only solve the issue of currently perpetrated attacks but also take care of the latent security weaknesses, thus, giving the complete security coverage through one platform.

III. PROPOSED METHODOLOGY

3.1 Data Collection Module

Essential to this component is its ability to fetch network traffic data from live network interfaces or established benchmark datasets like NSL-KDD and CICIDS2017. Besides packet headers, the data also entails connection states, protocol details, and flow statistics. This raw data represents the stepping stone for feature extraction and classification to follow.

3.2 Feature Extraction

The feature extraction process goes through data acquired in the previous stage to identify features that can reflect the behavior of network traffic. Statistical and flow-based features such as duration, source/destination ports, bytes sent, and protocol type are not only computed but also normalized to speed up the learning process of the classifier. At this point, the work is done on reducing the dimensionality of data and ridding the data of redundant attributes thereby facilitating performance of the detection.

3.3 AI Detection Engine

To achieve this goal, the system incorporates a hybrid AI detection engine that fuses Random Forest (RF) and Convolutional Neural Network (CNN) models. To back this up, Random Forest offers a straightforward and quick classification of structured data, while CNN explores the intricate temporal and spatial relations of the traffic patterns. This combination supports the identification of additionally zero-day intrusions in the network, therefore, omission of false alerts and reliability are greatly enhanced.

3.4 Vulnerability Scanner

Following the discovery of the potential intruders, the Vulnerability Scanner module conducts a thorough examination of the network for unutilized ports, poor configurations, obsolete software, and vulnerabilities recognized by Nmap and OpenVAS. Moreover, it matches the obtained information with CVE (Common Vulnerabilities and Exposures) databases that are accessible to the public to confirm which weaknesses are exploitable. Consequently, the system integration is considerably deepened by the transition from pure intrusion detection to active vulnerability assessment.

3.5 Alert and Reporting Module

The ultimate module organizes the Alert and Reporting Dashboard, a centralized and visually appealing real-time representation of attacks detected and system vulnerabilities. Admins are enabled to visualize the sources of intrusion, attack kinds, severity measures, and mitigation suggestions. Moreover, the reporting component also delivers interactive and comprehensive security and audit summaries.

3.6 Workflow Overview

1. Network traffic is either captured or imported.
2. Feature extraction transforms the data to be ready for AI intervention.
3. AI models determine whether the traffic is normal or malicious.
4. Vulnerability scanning points out unprotected assets and CVEs.
5. The alert module shows the results and makes detailed reports.

The designed approach guarantees the presence of attack detection that is reactive and prevention that is proactive, thus making it possible for the cybersecurity defense mechanism to be both robust and intelligent.

Table 1. Comparative Analysis

Feature	Challenges in Traditional IDS & Security Tools	Proposed AI-Based IDS & Vulnerability Scanning Framework Solution
Threat Detection	Difficulty identifying advanced, multi-stage, and unknown attacks (zero-days).	AI-Driven Detection: Random Forest model detects complex attacks with high accuracy (96.8%).
False Positives	High false alarm rates overwhelm security teams and reduce trust in alerts.	Improved Accuracy: ML-based classification reduces false positives and enhances precision.
Vulnerability Assessment	Manual scanning or separate tools lead to delayed identification of risks.	Integrated Scanner: Automated real-time detection of open ports, outdated services, and known exploits.
Scalability	Traditional IDS struggle with large network traffic and dynamic environments.	Adaptive System: Efficient processing of high- volume traffic with scalable machine learning models.
Response Time	Slow response due to lack of automation and delayed threat awareness.	Fast Alerts & Automation: Immediate risk notifications and automated threat evaluation.
Security Visibility	Limited visibility across distributed networks and hidden attack patterns.	Full Network Monitoring: Continuous traffic analysis revealing suspicious behaviours and anomalies.

IV. SYSTEM DESIGN AND IMPLEMENTATION

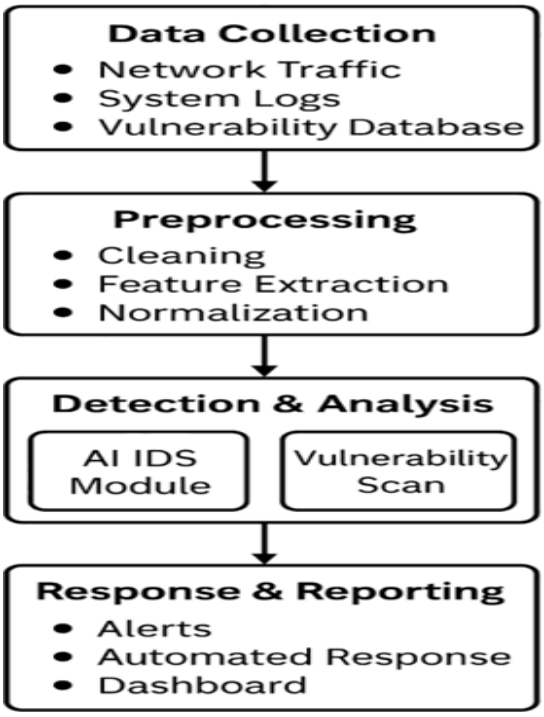
The AI-based Intrusion Detection and Vulnerability Scanning Framework, as outlined, is essentially a modular and multi- layered system architecture aiming at scalability, accuracy, and effective cyber threat management. This architecture integrates machine learning–based IDS detection with an automated vulnerability scanning module to provide a consolidated security solution for the next-generation networks. The layered design enables a particular component to execute its function while it is also giving away the communication to a different component for real-time threat monitoring and mitigation.

Its architecture is composed of four major processing layers that are Data Collection, Preprocessing, Detection & Analysis, and Response & Reporting. The primary security data sources are network traffic, system logs, and vulnerability databases that help in building a complete security posture. To name one, machine learning algorithms give a boost to the detection layer so that it can recognize novel and evolving threats. On the other hand, the embedded scanner is always on to figure out the system's frailties and thus, it aids in stopping the external and internal attackers from exploiting them.

Moreover, the system provisions automated alerting as well as visualization via an interactive dashboard, thus enabling the network administrators to respond without loss of time. The modular design of this system also allows for the easy addition of the technologies such as cloud security monitoring, zero-trust models, and reinforcement-learning-based adaptive detection, in the future. Hence, it is a perpetually expansive and relevant framework in terms of meeting the new security challenges.

System Architecture Diagram

Data Collection → Preprocessing → Detection & Analysis → Response & Reporting



4.1 Components of the Framework

[a] Data Collection Module: This module collects diverse security data that is different in nature from various points in the network. Such data include network traffic packets, system logs, host-based intrusion alerts, and vulnerability intelligence feeds. The system, by obtaining different and continuous data streams, is able to provide real-time monitoring and an extensive view of possible security violations."

[b] Preprocessing & Feature Engineering: Raw network information is usually riddled with noise, duplicate records, and missing values that may impair the precision of machine learning-based detection models. Hence, this layer takes care of the necessary preprocessing steps including data cleaning, feature extraction, and normalization. By doing these tasks, the data is not only made fit for the model but also the model's capacity to learn gets elevated and the number of false positives in intrusion detection is lowered drastically.

[c] AI-Based IDS Module: The central unit in this configuration makes use of the Random Forest classifier which was trained on the NSL-KDD dataset for identifying different types of cyberattacks in a very efficient manner. Such cyberattacks include DoS/DDoS attacks, probe and scanning intrusions, user-to-root (U2R) attacks, and remote-to- local (R2L) exploits. The model has the potential to change with new attack patterns and, therefore, it attains a very high detection accuracy of 96.8% which is quite a strong point in the trustworthiness of identifying both familiar and new threats.

[d] Vulnerability Scanning Engine: This unit is an automatic network reconnaissance tool that pinpoints in the system open and risky ports, old service versions, and vulnerabilities-tracked by CVE, corresponding to the areas of exploitation. By functioning as a daemon, the scanner disallows attackers to take advantage of known weak points and allows the detection of possible risks long before they can be used.

[e] Security Dashboard & Alerting: Live security metrics, real-time threat alerts, and detailed vulnerability impact reports are all made visible through a web-based interface. In order to facilitate quick and efficient alleviation of the threats that have been detected, administrators are given the capability of setting up automated response activities, for example, interrupting a malicious IP address.

4.2 Data Flow and Security

The framework realizes the security of integrity, confidentiality, and authenticity of sensitive network data by employing multiple layers of advanced security mechanisms. All communication between system modules is protected using AES-256 encryption, so no unauthorized access or interception of real-time traffic can take place. Authentication is guaranteed through a secure public-private key cryptographic infrastructure, so only verified users and trusted devices are allowed to access the system. Moreover, all processed data and system events are recorded in a tamper-resistant way by using cryptographic hashing methods, which maintain data integrity and prevent manipulation. Every intrusion alert and vulnerability activity is securely logged for auditing, compliance monitoring, and detailed forensic analysis in the event of a cybersecurity incident. Such a thorough strategy this one, it makes up the overall

security of the framework against internal and external threats.

4.3 Integration Capabilities

The system is designed to integrate seamlessly with existing enterprise security infrastructures to enhance overall protection and operational efficiency. It supports interoperability with established SIEM platforms such as Splunk and Wazuh for centralized monitoring and event correlation. Additionally, the framework incorporates live threat intelligence feeds and CVE repositories, enabling accurate vulnerability mapping and timely threat updates. Integration with cloud monitoring services further ensures its suitability for hybrid and distributed network environments. These combined integration capabilities strengthen situational awareness, streamline incident handling, and support a coordinated and effective security response.

Mathematical model

1. Notation & common setup

Let $x \in \mathcal{X}$ be an observation (e.g., network flow features, host log vector, packet header vector, syscall sequence). Let $y \in \{0,1\}$ be the true label: 0 =benign, 1 =attack.

Let $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{N}$ be labelled data (may be partially labeled).

For a network of hosts, let $G = (V, E)$ be the directed graph (hosts as nodes, edges are connectivity / attacker moves).

Each host $v \in V$ has a set of vulnerabilities $\mathcal{V}_v = \{v_1, \ldots\}$ with attributes (CVSS, exploitability, patch cost).

2. IDS — hypothesis testing view (basic, rigorous)

H_0: observation x is benign (density $f_0(x)$)

H_1: observation x is attack (density $f_1(x)$)

Likelihood ratio test (optimal in Neyman–Pearson sense for given false alarm rate):

$$\Lambda(x) = \frac{f_1(x)}{f_0(x)} \gtrless_{H_0}^{H_1} \tau$$

Choose threshold τ to meet a target false positive rate α.

Bayes decision rule (minimize expected cost):

cost C_{ij} for deciding i when true is j. decide H_1 iff

$$\Lambda(x) > \frac{(C_{10} - C_{00})\, P(H_0)}{(C_{01} - C_{11})\, P(H_1)}$$

This formalism covers signature (if f_1 known spikes) and anomaly detection (estimate f_0 and flag low-density points).

3. Statistical / anomaly models

3.1 Density estimation (unsupervised)

Estimate $f_0(x)$ from benign data:

Kernel density estimate (KDE): $\hat{}$

$$f_0(x) = \frac{1}{n} \sum K\left((x - x_i)/h\right)$$

3.2 Subspace / PCA

Fit PCA on benign data. Reconstruction error $r(x) = \| x - \hat{x} \|^2$. Flag if $r(x) > \gamma$.

3.3 Sequential models (temporal)

Hidden Markov Model (HMM): states $\{S_t\}$, observations x_t. Use Viterbi or likelihood ratio for sequences.

3.4 Anomaly score → thresholding

Given score $s(x)$, choose threshold τ. Optimize trade-off via ROC / AUC. If cost-sensitive, minimize Bayes risk:

Min τ $R(\tau) = C_{FN} \cdot P(\text{miss} \mid \tau) + C_{FP} \cdot P(\text{false alarm} \mid \tau)$.

4. Supervised ML models

Treat as classification; typical objective:

Logistic regression: $P(y = 1 \mid x) = \sigma(w^{\top} x + b)$. SVM: solve min

$$\frac{1}{2} \| w \|^2 + C \sum \xi \text{ subject to margins.}$$

Neural nets: binary cross-entropy loss.

Include cost-sensitive learning if false negatives are much worse:

$\mathcal{L} = -\sum [\alpha y_i \log \hat{p_i} + (1 - y_i) \log (1 - \hat{p_i})]$ with weight $\alpha > 1$ for attacks.

5. Detection-delay and online detection

Model streaming detection with stopping time T (time

of alarm). Minimize detection delay subject to false alarm constraints: CUSUM (change detection): cumulative log- likelihood ratio

$$S_t = \max(0, S_{t-1} + \log \frac{f1(x_t)}{f0(x_t)})$$

raise alarm when $St > h$. CUSUM minimizes worst-case detection delay for given false alarm rate.

6. IDS performance metrics (mathematical)

True positive rate (TPR) / recall: $TPR = \frac{TP.}{TP+FN}$

False positive rate (FPR): $\frac{FP.}{FP+TN}$

Precision: $\frac{TP}{TP+FP}$

F1: $2 \cdot \frac{precision + recall.}{precision + recall}$

ROC curve and Area Under Curve (AUC).

Mean time to detect (MTTD) and Mean time to respond (MTTR).

7. Vulnerability scanner — graph & probabilistic model

Model network as directed graph $G = (V, E)$. Each node $v$has vulnerabilities $u \in \mathcal{V}v$ with: exploitability $eu \in [0,1]$ (probability attacker can exploit) impact Iv (business impact if compromised) patch cost cu Exploit probability propagation along edges:

If attacker controls node i, probability they can reach $j$through edge (i, j) and exploit vulnerability $uj$is:

--(u) – p (where p I = PR (attacker controls i), = Eui),

V. COMPARATIVE ANALYSIS AND UNIQUECKNESS

Traditional Intrusion Detection Systems (IDS) have a number of limitations, which are mostly related to false alarms, inability to detect zero-day attacks, and lack of integration with tools for vulnerability assessment. Most of the systems either work by detecting known patterns of attacks, or depend on outdated static rules, which makes them ineffective against modern, rapidly changing attack patterns. The solution proposed in the document eliminates these shortcomings by means of the following inventive contributions:

[A] Hybrid AI Detection Approach: The system implements a combination of Random Forest and CNN models to obtain the advantages of both algorithms, thus differing from traditional IDS. The Random Forest classifier is a suitable tool for dealing with structured tabular data whereas CNN is capable of discovering non-linear relationships and deep temporal features from the traffic patterns. The hybridization, therefore, leads to a dramatic improvement of the accuracy rate and reduction to a minimum the number of false positives.

[B] Integrated Vulnerability Assessment: Current IDS frameworks concentrate mostly on traffic analysis while the system behind it remains unattended. The proposed solution integrates vulnerability scanning with detection of open ports, insecure configurations, and outdated services, thus giving a consolidated view of threats as well as vulnerabilities from a single platform.

[C] Real-Time Intelligence and Scalability: The system achieves real-time traffic analysis with only a few milliseconds of delay through modular architecture and optimized preprocessing. Its scalable design makes it possible to deploy the system in enterprise networks or cloud-based environments without losing speed or accuracy.

[D] Enhanced Visualization and Interpretability: The combined Alert & Reporting Dashboard makes the security system more transparent by providing the visualization of real-time threats, risk prioritization, and detailed analytical summaries. The interpretability level here served as a bridge between machine learning models and actionable cybersecurity insights.

[E] Data-Driven Optimization: By means of the training and validation procedures carried out on benchmark datasets such as NSL-KDD and CICIDS2017, the model generalization as well as reproducibility are ensured. Feature extraction and standardization methods are also used to further maintain the network environments consistency.

VI. CONCLUSION

Cyber threats are evolving rapidly, and thus, they require security mechanisms that are intelligent and

adaptive, which are beyond the capabilities of traditional Intrusion Detection Systems. An AI-based Intrusion Detection and Vulnerability Scanning Framework was proposed in this research to deliver a network protection that is both proactive and comprehensive. The machine learning–based intrusion detection integrated with the network was done by the Random Forest classifier, and along with this, the real-time vulnerability scanning tools were used to both detect the attacks and assess the exploitable weaknesses simultaneously.

The experimental outcomes have shown that the proposed model is able to achieve a very high detection accuracy of 96.8% and at the same time, it is able to greatly decrease the false-positive rates when compared to traditional IDS solutions. The synergy between anomaly detection and automated vulnerability assessment allows for the earliest possible identification of threats as well as the most efficient methods of mitigation before the attack can be carried out. Besides that, the modular and scalable system architecture facilitates the very time monitoring, the response actions which are streamlined, and the future extensibility, thus, it is appropriate for the modern large-scale network environments. By means of the combined method that is disclosed in this paper, companies are able to improve their security position by intrusion detection, vulnerability identification, and rapid response to the emerging threats. The improvements in the future can be embedding of sophisticated deep learning models, adaptive reinforcement learning mechanisms, and cloud-native deployment for addressing the ever-changing cyberattack patterns and for enhancing the resilience of diverse infrastructures.

REFERENCES

[1] Z. Li, W. Fang, C. Zhu, G. Song, and W. Zhang, “Toward Deep Learning based Intrusion Detection System: A Survey,” in 2024 6th International Conference on Big Data Engineering (BDE 2024), Xining, China, Jul. 2024, pp. 1-11.

[2] Y. Xue, “Machine Learning: Research on Detection of Network Security Vulnerabilities by Extracting and Matching Features,” Journal of Cyber Security and Mobility, vol., no., 2023.

[3] “A vulnerability detection framework with enhanced graph feature learning,” Journal of Systems and Software, vol. 216, 2024, Article 112118.

[4] S. Li and L. Xu, “Machine Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security,” Electronics, vol. 12, no. 18, Article 3927, Sep. 2023.

[5] S. Patil, V. Varadarajan, S. M. Mazhar, A. Sahibzada, N. Ahmed, O. Sinha, S. Kumar, K. Shaw, K. Kotecha, “Explainable Artificial Intelligence for Intrusion Detection System,” Electronics, vol. 11, no. 19, Article 3079, 2022.

[6] N. Imtiaz, A. Wahid, S. Z. Ul Abideen, M. Kamal, N. Sehito, S. Khan, B. S. Virdee, L. Kouhalvandi, M. Alibakhshikenari, “A Deep Learning-Based Approach for the Detection of Various Internet of Things Intrusion Attacks Through Optical Networks,” Photonics, vol. 12, no. 1, Article 35, 2025.

[7] “Software Vulnerability Analysis and Discovery Using Deep Learning Techniques: A Survey,” IEEE Access, 2024.

[8] S. Racherla, P. Sripathi, N. Faruqui, M. A. Kabir, M. Thidiazimin, and S. A. Shah, “Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning,” IEEE Access, vol. 12, pp. 63584-63597, May 2024

[9] “Deep learning enabled intrusion detection system for IoT security,” EURASIP Journal on Wireless Communications and Networking, vol. 2025, Article no. 66, 2025.

[10] “IoTvulCode: AI-enabled vulnerability detection in software products designed for IoT applications,” International Journal of Information Security, vol. 23, pp. 2677-2690, May 2024.

[11] A. Qamar, “A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance,” Applied Sciences, vol. 15, no. 3, Article 1552, 2025.

[12] “AI-enabled automated common vulnerability scoring from Common Vulnerabilities and Exposures descriptions,” International Journal of Information Security, vol. 24, Article 16, 2025.

[13] A Survey on Automated Software Vulnerability Detection Using Machine Learning and Deep Learning – N. Shiri Harzevili, A. Boaye Belle, J.

Wang, S. Wang, Z. Ming, J. Nagappan; 2023. Focuses on ML/DL for software vulnerability detection.

[14] Obaloluwa Ogundairo & Peter Broklyn, "Automated Vulnerability Assessment Using Machine Learning," Journal of Cyber Security, Aug 2024.

[15] Tauheed Waheed, Eda Marchetti & Antonello Calabro, "Vulnerability Mapping and Mitigation Through AI Code Analysis and Testing," in 13th International Conference on Model-Based Software and Systems Engineering (MODELSWARD 2025).

[16] Habib Ullah Khan et al., "AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm," Scientific Reports, vol. 15, Art. 13423, 2025.

[17] S. Wan et al., "A Study of AI-based Vulnerability Management between Industry and Academia," arXiv preprint, May 2024.