IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14661

"AI-Powered Intrusion Detection: Machine Learning for Harmful Packet Detection"

Mrs. Rajashree M Byalal[1], Shreyas M V[2], Rahul C[3], Rishika Lokesh[4], Vaishnavi A[5]

Guide, Department of Computer Science - ICB, K. S. Institute of Technology, Bengaluru, India[1]

Department of Computer Science - ICB, K. S. Institute of Technology, Bengaluru, India[2-5]

Abstract: In an era of increasing digital connectivity, the sophistication and frequency of cyberattacks have grown exponentially, rendering traditional rule-based intrusion detection systems (IDS) insufficient. This literature survey explores the recent advancements in AI-powered IDS solutions, with a particular focus on machine learning (ML)-driven approaches for harmful packet detection. The review analyzes 25 recent research papers published between 2020 and 2025, highlighting trends in model development, dataset utilization, real-time deployment, edge computing, and automation in threat response. While many existing systems achieve high detection accuracy using algorithms such as Random Forest, SVM, CNN, and ensemble techniques, they often fall short in critical areas—such as real-time performance, attack simulation, automated remediation, and handling minority class attacks. This survey identifies those gaps and establishes the motivation for a lightweight, modular IDS that not only detects but also responds to intrusions through intelligent patch recommendations. By comparing existing approaches and their limitations, the paper lays the foundation for building adaptive, scalable, and semi-autonomous security solutions suitable for modern network environments.

Keywords: Intrusion Detection System, Machine Learning, NSL-KDD, Network Security, Automated Patching, Real-Time Threat Detection, Cyberattack Classification, Lightweight IDS

I. INTRODUCTION

As the digital landscape continues to expand, so does the surface area for cyberattacks. From financial institutions to critical infrastructure, modern networks are constantly under threat from increasingly sophisticated intrusion attempts. Traditional Intrusion Detection Systems (IDS) that rely on predefined rules and signature-based detection have proven effective only against known attack patterns. However, they often fail to detect novel or evolving threats, resulting in delayed responses or complete oversight of malicious activity.

The growing complexity and frequency of cyberattacks have paved the way for intelligent, data-driven defense mechanisms. Among them, machine learning (ML) and artificial intelligence (AI) have emerged as powerful tools for designing adaptive IDS solutions. These systems are capable of learning from historical data, identifying hidden patterns in network traffic, and making real-time decisions without explicit human instruction. With datasets like NSL-KDD, researchers have been able to train models to detect and classify a wide range of attacks including Denial of Service (DoS), Probing, User-to-Root (U2R), and Remote-to-Local (R2L) exploits.

Despite these advancements, many ML-based IDS models remain limited in scope. They often operate in offline settings, lack real-time responsiveness, and rarely offer remediation once an attack is identified.

Moreover, the challenge of imbalanced datasets, feature redundancy, and computational overhead further complicate deployment in real-world environments. Few systems extend beyond detection to incorporate meaningful response mechanisms like security patching or rule reconfiguration.This literature survey aims to explore the current landscape of AI-powered IDS research, focusing on works published between 2020 and 2025. It critically analyzes 25 research papers categorized by model architecture, data handling, deployment strategy, and automation capabilities. The goal is to highlight what has been achieved, what gaps still remain, and how these insights inform the development of a more holistic, lightweight, and responsive intrusion detection system—one that doesn't just identify threats but also acts on them.

II. LITERATURE SURVEY

With the rapid advancement of networked systems and increasing reliance on digital infrastructure, the threat landscape has grown significantly. Intrusion Detection Systems (IDS) have become essential in identifying unauthorized or

DOI: 10.17148/IJARCCE.2025.14661

malicious activities within networks. However, traditional IDS solutions—often rule-based or signature-dependent—struggle to detect unknown threats, adapt to evolving attack patterns, or scale efficiently. In response, researchers have turned to artificial intelligence, particularly machine learning (ML), to develop more flexible, accurate, and intelligent IDS models.

This survey synthesizes findings from 25 peer-reviewed research papers published between 2020 and 2025. These works span a wide array of approaches, including supervised learning, deep learning, feature optimization, and emerging fields such as federated and edge-based intrusion detection. The goal is to understand the strengths and limitations of current systems and identify opportunities for improvement that will guide the development of the proposed AI-powered IDS.

2.1 Machine Learning Models for Intrusion Detection

Many studies have demonstrated the effectiveness of machine learning techniques in improving detection accuracy and reducing false positives. Common algorithms include Random Forest (RF), Support Vector Machines (SVM), Decision Trees (DT), and ensemble models like XGBoost and AdaBoost. These classifiers are frequently trained on benchmark datasets such as NSL-KDD, KDD'99, and UNSW-NB15 to identify attacks like DoS, Probe, U2R, and R2L.

Several works, such as those by Malik et al. and Alzahrani et al., focused on model optimization through feature selection techniques, including genetic algorithms and correlation-based filtering. These approaches help reduce model complexity while maintaining performance. Others explored deep learning methods, using CNNs and LSTMs for sequence analysis and time-based detection, often achieving high accuracy on multi-class classification tasks.

Despite strong performance in controlled settings, these models often struggle when exposed to real-time or imbalanced data. Rare attack types like U2R and R2L remain difficult to detect accurately, indicating a need for more balanced training and fine-grained classification strategies.

2.2 Real-Time and Edge-Based IDS

A growing trend in IDS research is the shift toward real-time, lightweight systems that can be deployed on edge devices or integrated into cloud-native environments. Papers by Zhang et al. and Bouzidi et al. highlighted the use of transformer-based and lightweight neural networks for efficient on-device inference. These approaches improve latency and reduce dependence on centralized infrastructure, making them ideal for modern, distributed network environments.

Edge computing also addresses privacy concerns, particularly in environments where sensitive data cannot be transmitted for centralized analysis. Federated learning, as proposed by Sun et al., enables collaborative model training across multiple nodes without sharing raw data. However, these approaches introduce new challenges in model synchronization, consistency, and increased implementation complexity.

2.3 Dataset Handling and Preprocessing Challenges

The quality and structure of the training dataset heavily influence model performance. While NSL-KDD remains a widely accepted benchmark due to its balanced and preprocessed nature, it still contains some redundancy and lacks real-time network traffic simulation. Many studies that use this dataset fail to implement advanced preprocessing pipelines, leading to suboptimal results or overfitting.

Feature selection and normalization techniques are essential in managing high-dimensional data and minimizing noise. Several papers emphasized the need for improved preprocessing to ensure model generalizability, especially for underrepresented classes. Techniques like SMOTE, one-hot encoding, and min-max normalization were commonly applied to enhance data usability.

2.4 Remediation and Automation Gaps

One of the most significant gaps observed in the literature is the lack of integrated response mechanisms. Most IDS solutions stop at detection and reporting, offering little to no guidance on how to mitigate the threat. Only a few studies explored rule-based or semi-automated remediation approaches, such as modifying firewall rules or generating response alerts.

This reactive approach leaves systems vulnerable during the time it takes for a human administrator to intervene. A truly intelligent IDS should not only detect threats but also offer—or execute—relevant countermeasures. This gap presents a strong opportunity for developing a system that couples ML-based detection with patch recommendation or automated configuration changes.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14661

2.5 Summary of Observations

The analysis of 25 recent research papers highlights the significant progress made in the field of AI-powered intrusion detection, particularly through the use of machine learning and deep learning techniques. Models such as Random Forest, SVM, CNN, and various ensemble methods have shown high accuracy in detecting common attack types and reducing false positives. Approaches involving edge computing and federated learning have also introduced promising pathways for scalable and privacy-preserving deployment. However, despite these advancements, several critical limitations persist. Many systems are not optimized for real-time execution or lightweight environments, making them impractical for real-world, resource-constrained networks. Moreover, most IDS solutions lack integrated response mechanisms, stopping at detection without offering actionable remediation or automated patching. Rare attack types like R2L and U2R are still difficult to classify accurately due to dataset imbalance and inadequate feature representation. These gaps underscore the need for an IDS that not only classifies threats effectively but also simulates real-world attacks, adapts to changing environments, and recommends or deploys security patches. Addressing these issues is the driving force behind the development of the proposed AI-powered intrusion detection system with automated remediation capabilities.

III. SYSTEM REQUIREMENTS

The system requirements for the AI-powered Intrusion Detection System (IDS) are designed to support efficient data analysis, real-time detection, and seamless integration with existing network infrastructures. To ensure smooth operation, a standard personal computer with at least an Intel i5/i7 or equivalent AMD processor, 8 GB of RAM (16 GB recommended for larger datasets), and a minimum of 256 GB SSD storage is required, ensuring enough space for datasets and logs. A CUDA-compatible GPU is optional for accelerating deep learning models but is not mandatory. The software environment is based on Python 3.10 or higher, with essential libraries like scikit-learn, pandas, NumPy, and joblib for machine learning, and visualization tools like Matplotlib and Seaborn for reporting results. For capturing and analyzing network packets, tools such as Wireshark and tcpdump are recommended, while Flask or FastAPI can be utilized to deploy the detection models as APIs.

The NSL-KDD dataset is the primary source of training and testing data due to its improved balance and reduced redundancy compared to KDD'99, though datasets like UNSW-NB15 or CICIDS2017 may be explored for transfer learning or robustness testing.To simulate network traffic and potential attacks, tools like Metasploit Framework (optional) or custom scripts can be employed in isolated virtual environments using platforms like VirtualBox or VMware.

Additionally, the system architecture includes the possibility of cloud deployment using services like AWS EC2 or Google Colab to handle scalability and heavier workloads. This comprehensive set of requirements ensures that the IDS project is both technically feasible and adaptable for future expansions, whether deployed locally, on the cloud, or within edge computing environments.

IV. PROPOSED METHODOLOGY

The proposed methodology for this AI-powered Intrusion Detection System (IDS) with automated security patching is designed to blend machine learning-based detection with real-time network monitoring and practical remediation strategies. The approach begins with the acquisition of network traffic, either through packet capturing tools like Wireshark or by utilizing pre-existing datasets such as NSL-KDD.

Once the data is collected, it undergoes a thorough preprocessing phase where irrelevant or redundant features are removed, categorical features are encoded numerically, and continuous features are scaled to ensure uniformity across the dataset.

Following this, a machine learning model—such as Random Forest or Support Vector Machine—is trained on the pre processed dataset to classify traffic into normal or various attack categories including DoS, Probe, R2L, and U2R. The model is then validated using techniques like cross-validation to assess its accuracy and robustness.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14661

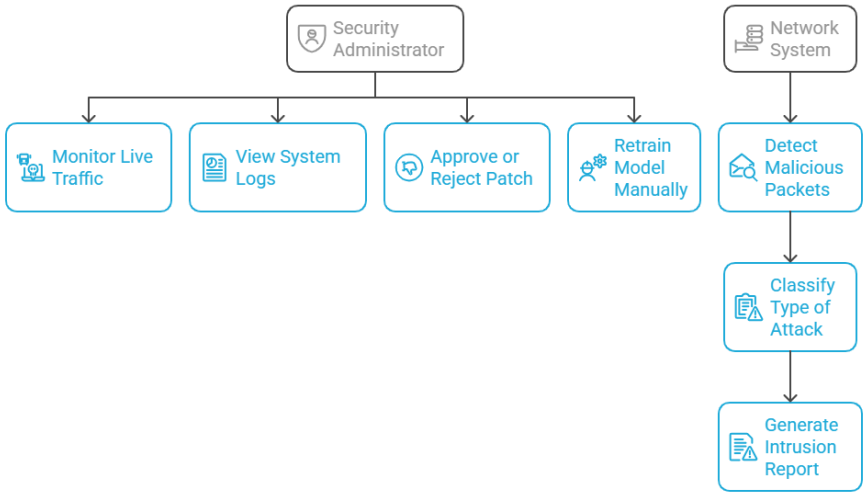

Figure: Network Security System Flowchart

After the model training, the system is deployed in a modular architecture that enables real-time traffic analysis. Incoming packets are continuously monitored and passed through the trained model for classification. Once an intrusion is detected, the system triggers an alert and logs the details, including attack type and confidence score. The most innovative aspect of this methodology is its integration of an automated patch recommendation module. This component analyzes the detected attack type and suggests appropriate security measures—such as updating firewall rules, applying patches, or isolating affected systems. For critical threats, administrators can review and approve these patches via a web-based dashboard, ensuring a human-in-the-loop approach to maintain oversight. Throughout the methodology, emphasis is placed on lightweight implementation and modular design to facilitate easy deployment across various environments, including edge devices and cloud platforms. This holistic approach not only enhances detection capabilities but also bridges the gap between threat detection and response, aligning the system closely with real-world security needs.

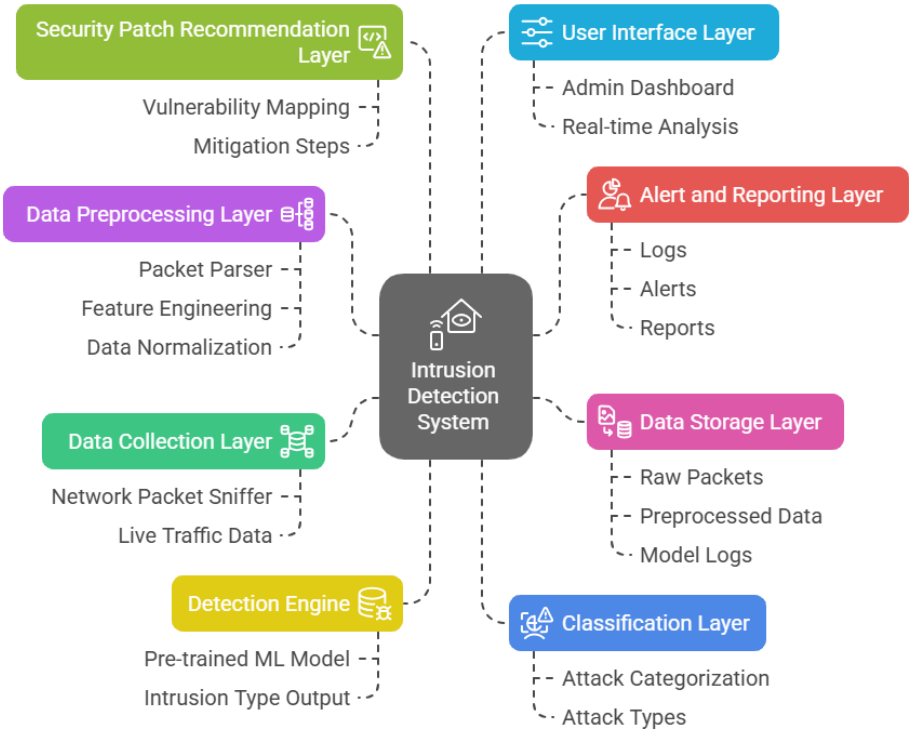

Figure: Block Diagram of System Architecture

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14661

V. CONCLUSION AND FUTURE SCOPE

In conclusion, this literature survey highlights the growing role of artificial intelligence in enhancing the capabilities of intrusion detection systems. The review of 25 recent research papers reveals that while significant strides have been made in applying machine learning algorithms—such as Random Forest, SVM, and deep learning models—to detect various types of attacks, several limitations still persist. Many systems focus heavily on detection accuracy without addressing real-time implementation challenges, resource efficiency, or automated remediation. Furthermore, issues like class imbalance, dataset quality, and the lack of robust response mechanisms continue to hinder the effectiveness of many current solutions.To address these gaps, our proposed AI-powered intrusion detection system aims to build on existing research by integrating lightweight models with real-time packet analysis, ensuring efficient detection even in resource-constrained environments.

By simulating attacks and validating the system under realistic network conditions, the project enhances its adaptability and robustness. Additionally, the inclusion of an automated security patching module bridges the gap between detection and response, reducing the time between threat identification and system remediation. This holistic approach aims to create a modular, scalable, and practical solution that is not only effective in detecting known and unknown threats but also in recommending or applying countermeasures.Looking ahead, future work could focus on expanding the system's scope by incorporating live traffic from diverse sources and integrating zero-trust architecture principles for enhanced security.

The adoption of federated learning could enable collaborative model training across distributed nodes while preserving data privacy. Moreover, exploring the use of adaptive reinforcement learning algorithms could empower the system to evolve in real-time, learning from new attack patterns and continuously refining its detection and response capabilities. These advancements will further strengthen the system's resilience, ensuring its relevance in increasingly complex and dynamic network environments

REFERENCES

[1] M. Nakıp and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," *arXiv preprint*, Jun. 2023.
[2] J. Lin, Y. Guo, and H. Chen, "Intrusion Detection at Scale with the Assistance of a Command-line Language Model," *arXiv preprint*, Apr. 2024.
[3] X. Yuan et al., "A Simple Framework to Enhance the Adversarial Robustness of Deep Learning-based Intrusion Detection System," *arXiv preprint*, Dec. 2023
[4] T. Ali and P. Kostakos, "HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs)," *arXiv preprint*, Sep. 2023.
[5] J. Ling et al., "Machine Learning-Based Multilevel Intrusion Detection Approach," *Electronics*, vol. 14, no. 2, p. 323, 2025.
[6] J. Feng, "Improved Machine Learning-based System for Intrusion Detection," in *Proc. ICIAAI 2024*, Oct. 2024.
[7] G. Sirisha et al., "An Innovative Intrusion Detection System for High-Density Communication Networks Using Artificial Intelligence," *Eng. Proc.*, vol. 59, no. 1, Dec. 2023.
[8] M. Al Lail et al., "Machine Learning for Network Intrusion Detection—A Comparative Study," *Future Internet*, vol. 15, no. 7, p. 243, Jul. 2023.
[9] A. Bhardwaj and S. S. N. Krishnan, "Intrusion Detection System Using Machine Learning," *IJERT*, Nov. 2023.
[10] Z. Sun et al., "Advancements in Training and Deployment Strategies for AI-based Intrusion Detection Systems in IoT: A Systematic Literature Review," *Journal of Cloud Computing*, 2025
[11] M. Cate, "AI-Powered Intrusion Detection Systems: Challenges and Opportunities," *ResearchGate*, Jan. 2025.
[12] "Evaluating Machine Learning-Based Intrusion Detection Systems with Explainable AI," *Frontiers in Computer Science*, 2025.
[13] "Advanced AI-Powered Intrusion Detection Systems in Cybersecurity," *Procedia Computer Science*, 2025.
[14] "Intrusion Detection System Based on Machine Learning Using Least Squares Support Vector Machine," *Scientific Reports*, 2025.
[15] "AI-Powered Intrusion Detection System for Network Security Using Supervised Classifiers," in *Ganitara Conf. Proc.*, 2025
[16] "AI-Based Intrusion Detection & Prevention Models for Smart Home IoT Systems: A Literature Review," *ResearchGate*, 2025.
[17] "A Comprehensive Review of AI-Based Intrusion Detection Systems," *ResearchGate*, 2025
[18] "A Comprehensive Systematic Review of Intrusion Detection Systems," *Journal of Engineering and Computation*, 2025.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14661

[19] "Explainable Artificial Intelligence Models in Intrusion Detection Systems," *Engineering Applications of Artificial Intelligence*, 2025.
[20] "Robust Intrusion Detection System with Explainable Artificial Intelligence," *arXiv preprint*, 2025.
[21] H. Sun et al., "Federated Learning-Based Intrusion Detection System for Smart IoT Environments," *IEEE Internet of Things J.*, Mar. 2024.
[22] K. Al-Rimy et al., "Intrusion Detection Using Attention-Based Convolutional Neural Networks," *Computers & Security*, Feb. 2024.
[23] F. Zhang and A. Rehman, "Real-Time Network Intrusion Detection Using Transformer-Based Deep Learning Models," *J. Netw. Comput. Appl.*, Apr. 2024.
[24] S. Dutta and N. Sharma, "Adaptive Intrusion Detection Using Hybrid Ensemble Deep Learning," *Electronics*, Jul. 2023.
[25] A. Zargar and L. Bouzidi, "Enhancing Intrusion Detection in Edge Computing Using Lightweight AI Models," *Future Generation Computer Systems*, Jan. 2025.