iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76621

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

AI-Driven: Network Intrusion Detection Systems

Amal Murali[1], Dharvish K. S.[2], Fasil Shah T. S.[3], Sreedil V. J.[4], Mahshiya V. M.[5]
[1, 2, 3, 4]*Department of Computer Science and Engineering, Universal Engineering College, Thrissur, Kerala, India*
[5]*Assistant Professor Department of Computer Science and Engineering, Universal Engineering College, Thrissur, Kerala, India*

Abstract: ***Modern computer networks, particularly those sup- porting Internet of Things (IoT), cloud, and edge environments, are increasingly exposed to sophisticated cyber-attacks such as zero-day exploits and stealthy intrusion techniques. Traditional Intrusion Detection Systems (IDS) primarily rely on signature- based or rule-based mechanisms, which limits their effective-ness against evolving threats. Recent advancements in Artificial Intelligence (AI) and Deep Learning (DL) have enabled IDS to automatically learn complex patterns from network traffic, significantly improving detection capability.***

This review paper presents a comprehensive survey of AI-driven IDS frameworks, focusing on deep learning, self-supervised learning, graph-based models, and hybrid approaches. Particular attention is given to recent trends addressing key limitations of existing systems, including lack of robustness to adversarial attacks and limited explainability of model decisions. Techniques such as adversarial training and Explainable Artificial Intelligence (XAI) are reviewed for their role in improving system reliability and analyst trust. The paper highlights challenges such as dataset imbalance, adversarial vulnerability, and scalability issues, and discusses future research directions for developing adaptive, reliable, and transparent intrusion detection systems suitable for modern network environments.

Index Terms: ***Intrusion Detection Systems, Artificial Intelligence, Deep Learning, Explainable AI, Adversarial Robustness, Network Security.***

I. INTRODUCTION

In today's hyper-connected digital environment, cybersecurity threats have become increasingly sophisticated, dynamic, and frequent. The rapid expansion of cloud computing, Internet of Things (IoT), and 5G networks has resulted in massive volumes of heterogeneous network traffic, significantly increasing attack surfaces. Intrusion Detection Systems (IDS) play a vital role in monitoring network behavior and identifying malicious activities that may indicate unauthorized access or cyber-attacks.

Traditional IDS approaches, including signature-based and rule-based systems, are effective in detecting known attack patterns but struggle to identify zero-day attacks and evolving threat behaviors. These systems depend heavily on predefined rules and historical signatures, limiting their adaptability. As a result, researchers have increasingly adopted Artificial Intelligence (AI) and Machine Learning (ML) techniques to improve intrusion detection accuracy and generalization.

Early machine learning-based IDS models such as Decision Trees, Support Vector Machines, and Random Forests achieved promising results but relied heavily on manual feature engineering. These approaches often struggled with high- dimensional data, class imbalance, and scalability issues. The emergence of deep learning has transformed IDS research by enabling automatic feature extraction and hierarchical pattern learning directly from raw network data.

II. LITERATURE SURVEY

This section reviews significant research contributions in AI-driven Intrusion Detection Systems, highlighting the evo- lution from traditional machine learning models to modern deep learning, self-supervised, and hybrid architectures.

Early studies compared classical supervised learning algo- rithms for IDS applications and demonstrated the effectiveness of ensemble methods such as Random Forests on benchmark datasets. Subsequent research introduced deep learning-based IDS models that combine Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) architectures to capture both spatial and temporal traffic patterns.

Several studies emphasized challenges related to dataset im- balance, redundancy, and lack of realistic attack diversity. To address these limitations, self-supervised and semi-supervised IDS frameworks were proposed, enabling models to learn from unlabeled or partially labeled data. Adversarial robustness has emerged as a critical research area due to the vulnerability of deep learning models to evasion and poisoning attacks. Adversarially regularized autoencoders and robust training strategies have been proposed to enhance IDS resilience. In parallel, lightweight IDS architectures have been developed for IoT environments, emphasizing efficiency and scalability.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Explainable Artificial Intelligence (XAI) has also gained attention in IDS research. Techniques such as SHAP-based feature attribution enable transparency by explaining model decisions, improving trust and interpretability for security analysts.

III. COMPARATIVE ANALYSIS AND DISCUSSION

The progression of IDS technologies demonstrates a shift from static, rule-based systems to adaptive, data-driven frame- works. Deep learning-based IDS models outperform traditional approaches by learning complex non-linear patterns in network traffic. CNNs effectively capture spatial feature correlations, while RNN-based models such as LSTM and GRU excel in modeling sequential traffic behavior.

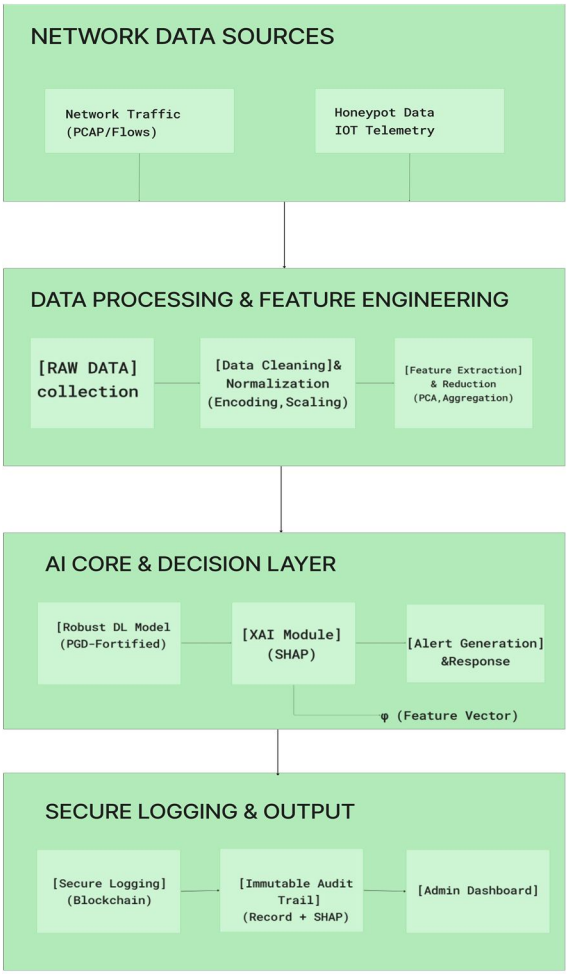


Fig. 1. General architecture of AI-driven Intrusion Detection Systems

Hybrid frameworks that integrate deep learning with traditional classifiers improve generalization, particularly when la- beled data is limited. Adversarial training techniques introduce defensive mechanisms that mitigate evasion attempts, enhanc- ing system reliability. Explainability further strengthens IDS deployment by enabling analysts to understand and validate intrusion alerts.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. CONCLUSION

This review surveyed recent advancements in AI-driven Intrusion Detection Systems, focusing on deep learning, self-

TABLE I
COMPARISON OF MAJOR AI-DRIVEN IDS FRAMEWORKS

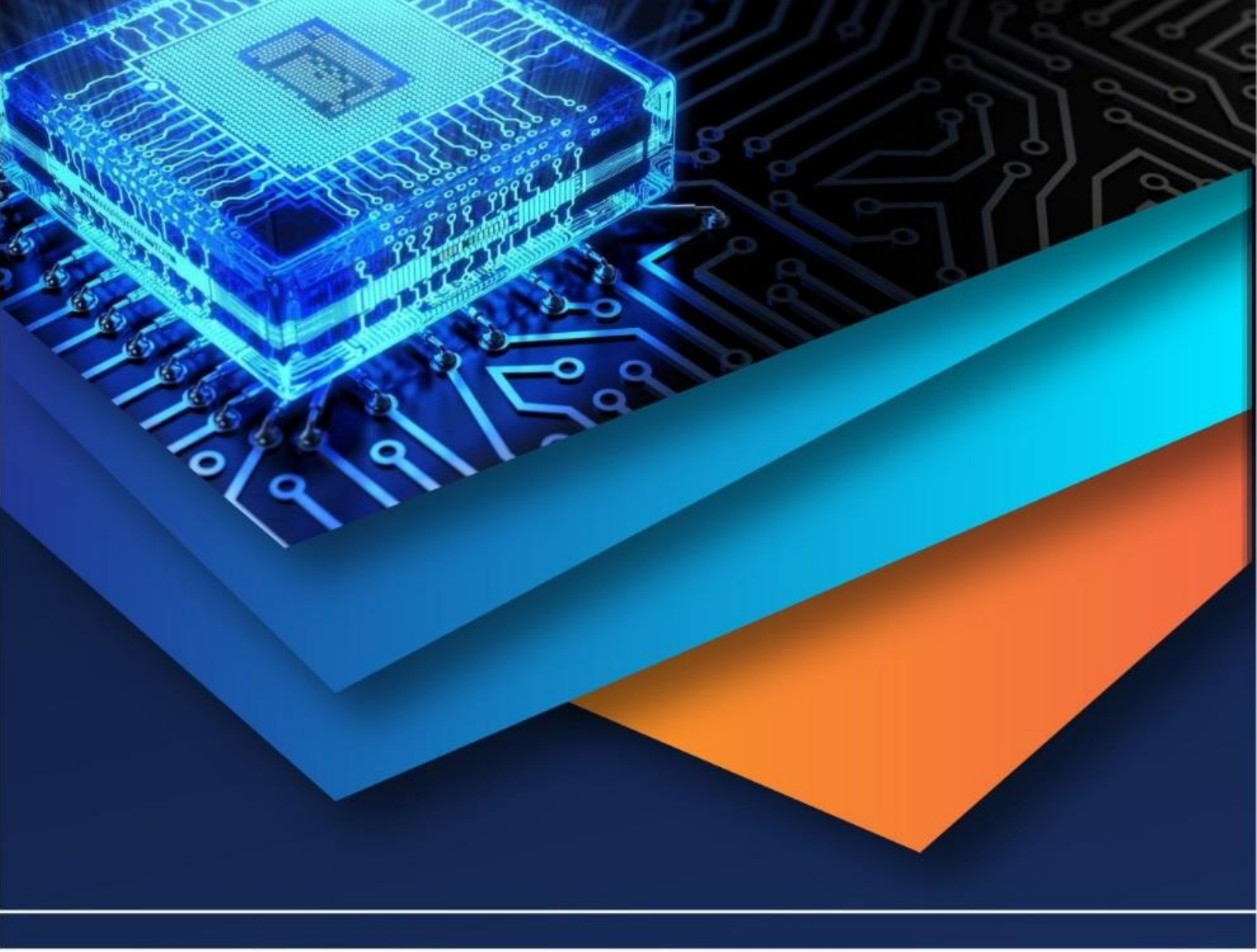
Model	Accuracy (%)
CNN–LSTM IDS	98.7
DOC-IDS	99.1
SAFE	97.4
ARCADE	96.8
EIDM	98.3
E-GraphSAGE	98.1
Explainable RF-IDS	95.0
GAN-IDS	98.6

supervised learning, explainability, and adversarial robustness. Deep learning architectures such as CNNs, RNNs, Autoen- coders, and Graph Neural Networks have significantly en- hanced IDS performance by learning complex traffic repre- sentations.

Despite notable progress, challenges remain in address- ing dataset imbalance, adversarial vulnerability, computational overhead, and privacy concerns. Future research should ex- plore federated and privacy-preserving IDS models, scalable architectures for IoT environments, and interpretable AI tech- niques for real-world deployment. Overall, AI-driven IDS represent a crucial step toward intelligent, adaptive, and trust- worthy cybersecurity defense systems.

REFERENCES

[1] A. Kumar and S. Yadav, "Evaluation of Machine Learning Algorithms for Intrusion Detection System," 2021.
[2] R. Singh and A. Gupta, "AI-Driven Intrusion Detection Systems: Lever- aging Deep Learning for Network Security," IEEE Access, 2022.
[3] K. Mehta and D. Sharma, "A Comparative Study on AI-IDS Artificial Intelligence-Based Intrusion Detection System," International Journal of Computer Applications, 2023.
[4] H. Patel and R. Reddy, "A Comprehensive Review of AI-Based Intrusion Detection Systems," Computers Security, 2023.
[5] M. Khan et al., "DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic," IEEE Access, 2022.
[6] Y. Zhang et al., "SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection," Expert Systems with Applications, 2023.
[7] J. Lee and K. Park, "ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection," Computers Security, 2024.
[8] T. Rahman and P. Sharma, "EIDM: Deep Learning Model for IoT Intrusion Detection Systems," Sensors, 2024.
[9] A. Sinha and N. Patel, "Explainable AI and Random Forest Based Reliable Intrusion Detection System," IEEE Transactions on Information Forensics and Security, 2022.
[10] M. Nakıp and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," arXiv preprint arXiv:2303.11245, 2023.
[11] H. Xu and W. Lin, "E-GraphSAGE: A Graph Neural Network Based Intrusion Detection System for IoT," arXiv preprint arXiv:2106.11705, 2021.
[12] E. Caville et al., "Anomal-E: A Self-Supervised Network Intrusion Detection System Based on Graph Neural Networks," arXiv preprint arXiv:2206.01783, 2022.
[13] R. Thomas and A. Banerjee, "Adversarial Robust and Explainable Net- work Intrusion Detection Systems Based on Deep Learning," Computers Security, 2023.
[14] M. Qureshi and B. Singh, "Enhancing Network Intrusion Detection Performance Using Generative Adversarial Networks," IEEE Access, 2023.
[15] J. Zhao et al., "CSAGC-IDS: A Dual-Module Deep Learning Network Intrusion Detection Model for Complex and Imbalanced Data," Infor- mation Sciences, 2024.
[16] L. Wang and S. Kim, "Network-Based Intrusion Detection Using Deep Learning Technique," Scientific Reports, Nature Publishing Group, 2025.
[17] V. Roy and S. Das, "Machine Learning-Based Network Intrusion Detec- tion for Big and Imbalanced Data Using Oversampling, Stacking Feature Embedding and Feature Extraction," Future Generation Computer Sys- tems, 2023.
[18] T. Kumar et al., "A Systematic Literature Review of Methods and Datasets for Anomaly-Based Network Intrusion Detection," IEEE Ac- cess, 2021.
[19] R. Singh and K. Jain, "Optimized IoT Intrusion Detection Using Machine Learning Technique," Wireless Networks, 2023.
[20] C. Huang et al., "An Adaptable Deep Learning-Based Intrusion De- tection System to Zero-Day Attacks," arXiv preprint arXiv:2109.14523, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)