Intelligent Intrusion Detection Systems for Mitigating Cyber Attacks: A Comprehensive Review

Rahul Rajendra Papalkar[1], Dr. Sanjay Kumar Singh[2]

[1]Lincoln University College Malaysia, Vishwakarma University Pune.
rahul.papalkar@vupune.ac.in
[2]Amity Institute of Information technology, Amity University Uttar Pradesh,
Lucknow Campus
sksingh1@amity.edu

Abstract

As the digital world continues to grow more integrated, so too are the threats to cybersecurity, including Distributed Denial of Service (DDoS) and botnet attacks, which are among the most concerning. These attacks harness already compromised digital devices which flood the target with traffic, making them exceedingly difficult to detect and mitigate with standard Intrusion Detection Systems (IDS). The current review examines the state of the art in intelligent and adaptive IDS with a focus on machine learning (ML) and deep learning (DL) algorithms and hybrid feature selection that alleviate the systems weaknesses to DDoS and botnet assaults. The author analyzes models based on ensemble learning methods, including Random Forest (RF), XGBoost, and LightGBM, as well as advanced deep learning with Convolutional Neural (CNN) and Long Short-Term Memory (LSTM) networks, in relation to the CIS-DDoS2019, CTU-13, and BoT-IoT datasets. In addition to the essential complement of real-time detection and adaptive anomaly detection, the feedback loops in systems which are essential to mounting a defense to the multiple and ever-changing aspects of cyber threats are discussed. There is a focus on understanding and analyzing the issues connected to the relevance of research, such as scalability, false positive reduction, adversarial resilience, and the challenges of implementation in diversified IoT and cloud environments. Furthermore, the review identifies the integration of Software Defined Networking (SDN) and federated learning for privacy-preserving and collaborative threat detection as possible future avenues. This review provided a comprehensive and balanced overview of intelligent IDS systems by juxtaposing the current developments with the existing gaps, offering valuable insights for both scholars and practitioners working on cyber security systems that are adaptive, resilient, and scalable. Therefore, responding to the questions posed in the review will necessitate considerable ingenuity.

Keywords: Intrusion Detection Systems, DDoS, Botnet Attacks, Machine Learning, Deep Learning, Anomaly Detection

Introduction:

The rise of the Internet of Things (IoT), cloud computing, mobile applications, and high-speed communication has led to increased integration of the digital world. However, along with these technological advancements, new cybersecurity challenges have emerged. Distributed Denial of Service

(DDoS) and botnet attacks have become major threats, causing significant financial and reputational damage. These attacks are particularly difficult to mitigate using traditional Intrusion Detection Systems (IDS), as they leverage compromised devices to flood networks with traffic, making it harder to distinguish between legitimate and malicious activity. This review aims to evaluate the state of intelligent IDS, focusing on Machine Learning (ML) and Deep Learning (DL) techniques, which offer promising solutions to improve the detection of such attacks. The review examines various IDS models and highlights the potential of using hybrid feature selection techniques and feedback loops to enhance detection capabilities.

➢ **Need for Intelligent IDS:**

Traditional IDS methods have been insufficient in detecting modern-day attacks, particularly DDoS and botnets. One of the primary issues is the inability of these systems to recognize new attack signatures, handle encrypted traffic effectively, and reduce false positives. In response to these challenges, ML and DL technologies have shown promise. Techniques such as Random Forest, XGBoost, and LightGBM are known for their robustness and generalization capabilities. Furthermore, Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks are particularly effective in learning complex patterns in network traffic. By combining hybrid feature selection methods with advanced detection algorithms, these systems can be adapted to mitigate the weaknesses of traditional IDS, particularly in real-time and dynamic environments.

➢ **Research Challenges:**

The development of intelligent IDS has led to significant improvements, but challenges remain. These challenges include:

- High False Positives: Many IDS models struggle to distinguish between legitimate and malicious traffic, leading to an increased number of false alarms.
- Real-time Adaptability: Many existing IDS solutions struggle to maintain performance under high traffic volumes, particularly in diverse environments such as IoT and cloud computing.
- Evasion Resilience: Attackers continually evolve their methods to mimic legitimate traffic, making it difficult for IDS to detect new attack vectors.
- Scalability and Cost: Some advanced IDS methods require significant computational resources, making them unsuitable for deployment in resource-constrained environments.

A scalable and efficient IDS framework that integrates feature engineering, ensemble learning, anomaly detection, and adaptive feedback loops could address these challenges.

➢ **Objective of the Review:**

This review aims to:

1. Analyze the role of ML and DL in the development of intelligent IDS, particularly for DDoS and botnet attacks.
2. Examine the effectiveness of ML and DL algorithms such as Random Forest, XGBoost, CNN, and LSTM in detecting attacks.
3. Assess the challenges related to scalability, false positive rates, and the time-sensitive nature of IDS.
4. Discuss the lack of research in adaptive and lightweight IDS solutions for encrypted traffic.

- **Contributions of This Review:**

This review synthesizes advancements in intelligent IDS by focusing on machine learning and deep learning techniques for attack detection. The review also provides insights into hybrid feature selection methods and how they improve the accuracy of IDS. It compares detection models based on ensemble learning methods such as Random Forest, XGBoost, and LightGBM, as well as advanced DL models like CNN and LSTM. The review also identifies key research gaps, including the challenges of scalability, real-time detection, and privacy concerns in IoT and cloud environments. Furthermore, the review highlights the need for future work on integrating Software Defined Networking (SDN) and federated learning to enhance the privacy-preserving capabilities of IDS.

Literature Review:

The literature on IDS has traditionally distinguished between two major approaches: signature-based IDS and anomaly-based IDS. While signature-based IDS is effective for detecting known attacks, it struggles with detecting novel threats. Anomaly-based IDS, on the other hand, aims to identify abnormal patterns in network traffic, but it too has limitations, particularly with high false positive rates and the inability to detect encrypted traffic.

Recent developments have focused on using ML and DL to overcome these challenges. The review highlights various works in the field that have shown how supervised and unsupervised learning techniques, particularly Random Forest, SVM, CNN, and LSTM, improve detection capabilities in complex network environments.

Ref	Technique Used	Dataset(s)	Results Obtained	Limitations	Future Scope
[1]	Supervised ML (RF, SVM)	IoT benchmark datasets	High detection accuracy, reduced FPR	Scalability issues	Adaptive real-time models
[2]	Lightweight ML with feature reduction	CIC-IDS2017, BoT-IoT	High accuracy, low latency	Struggles with encrypted traffic	Combine DL + XAI
[3]	Deep Learning (CNN, LSTM)	CIC-IDS2017	Robust classification	High computational cost	Model compression & pruning
[4]	Deep Neural Networks	UNSW-NB15	High detection, reduced false alarms	Overfitting, long training	Ensemble & data balancing
[5]	ML (RF, Gradient Boosting)	ISP-scale traffic	Strong real-time botnet detection	Poor adaptation to unseen botnets	Transfer learning, FL
[6]	Feature engineering + ML (DT, SVM)	CIC-IDS2017	High precision	Feature dependency	Raw packet analysis
[7]	Hybrid DL (CNN + LSTM)	NSL-KDD	Improved detection	Outdated dataset	Validation on real SDN traffic
[8]	Systematic review of ML for SDN botnet detection	CIC-IDS2017, CTU-13	Identified strengths of ML	Scalability & explainability gaps	FL & unsupervised models

[9]	Supervised ML (GB, RF)	UNSW-NB15	High accuracy, low false alarms	Training overhead	Incremental learning
[10]	Lightweight ML + feature selection	BoT-IoT	Efficient, accurate	Dataset-dependent features	Adaptive feature selection
[11]	Federated Learning (privacy-preserving)	IoT datasets	Good accuracy, privacy preserved	Communication overhead	Blockchain-secured FL

Research Methodology:

The paper describes the process of conducting a systematic review, starting with formulating research questions and conducting a scoping review to identify relevant literature. The methodology includes searching databases, screening titles and abstracts, evaluating the quality of selected articles, and analyzing the data extracted from these studies. The review focuses on IDS frameworks built using ML and DL algorithms and compares their performance based on standard datasets such as CIC-IDS2019, CTU-13, and BoT-IoT.

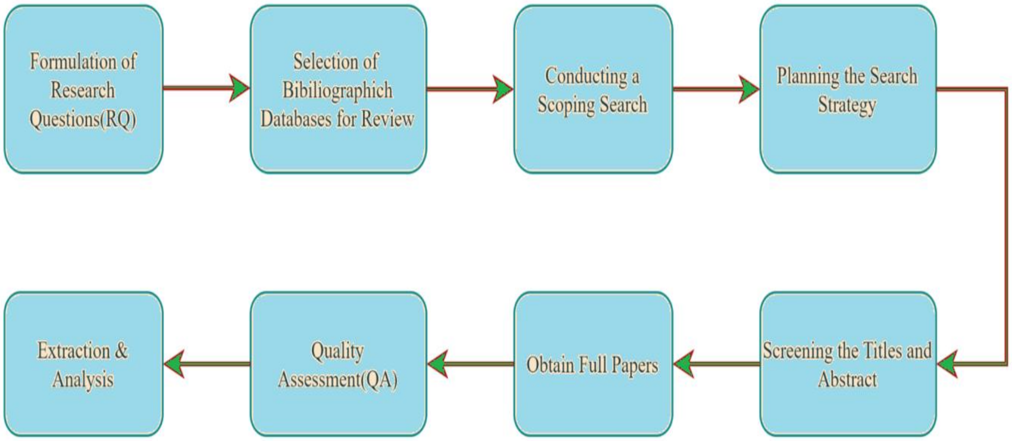
Formulation of Research Questions(RQ)
Selection of Bibiliographich Databases for Review
Conducting a Scoping Search
Planning the Search Strategy
Screening the Titles and Abstract
Obtain Full Papers
Quality Assessment(QA)
Extraction & Analysis

Figure 1: Process of Conducting a Systematic Review

***Discussion*:**

With more businesses embracing cloud computing, the importance of having the right security measures in place has also increased due to the higher risk of cyberattacks. There is, indeed, a need for more effective measures. AI's Intrusion detection systems (IDS) hold the capacity to lower the risks posed by cyberattacks through proper identifying and categorizing of cyber threats. The main function of an IDS is to monitor the flow of data in a network and alert the user when it detects any activities that require user attention. The amount of security traffic cloud systems and infrastructures need to deal with is unprecedented and poorly executed. IDS systems can identify intrusions using either approach. Binary classification, where the system identifies data as either normal or an attack, and multiclass classification, where the system identifies and categorizes multiple different attacks. Intrusion detection systems, with or without prevention capabilities, can be classified as signature based or an anomaly based. While the former is based on identifying patterns, the latter is based on abnormal behavior. Although the two systems serve unique purposes and play an important role in identifying intrusions, they are ineffective on their own when novel attacks are introduced. Unlike traditional security systems, the latest systems using machine learning (ML) and deep learning (DL) models perform with more efficiency. As a branch of artificial intelligence, machine learning (ML) utilizes supervised and unsupervised learning techniques to identify anomalies within network traffic. Relatively speaking, machine learning enhances performance and more sophisticated deep learning techniques arguably enhances prediction accuracy, thus, advanced deep learning techniques become more valuable for advanced intrusion detection systems. In this context, we analyze and review the comparative writings on AI-based intrusion detection systems, focusing on systems incorporating ML, deep learning (DL), and ensemble techniques. We also review comparative literature on the frameworks and approaches along with their descriptive and theoretical measures in the domain of observations and measures of cybersecurity, thus acting as a resource to others in the field.

Despite the promising results from advanced IDS methods, several challenges remain. A key issue is the high computational cost associated with deep learning models such as CNN and LSTM, which makes them unsuitable for real-time applications and for use in resource-constrained environments like IoT. There is also a need for better feature selection methods that can be dynamically adapted to changing network conditions. Furthermore, current IDS models often fail to generalize to new, unseen attack patterns, particularly in the case of zero-day attacks.

Future research must focus on optimizing IDS models for real-time detection in high-traffic environments, improving model generalization, and reducing false positives. There is also a need for adaptive feature selection techniques that can handle the evolving nature of network traffic.

Conclusion:

The growing sophistication of DDoS and botnet attacks necessitates the development of intelligent IDS that can detect and mitigate these threats in real-time. While current ML and DL-based IDS have shown promise, challenges related to scalability, real-time adaptability, and false positive reduction must be addressed. This review highlights the need for lightweight and adaptive IDS solutions, particularly for IoT and cloud environments. Future research should explore the integration of SDN and federated learning to enhance the privacy-preserving capabilities of IDS and improve their scalability. By overcoming these challenges, intelligent IDS will be better equipped to address the evolving landscape of cyber threats.

***References*:**

1. *Abiramasundari, S., & Ramaswamy, V. (2025). Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms. Scientific Reports, 15, Article 13098. https://doi.org/10.1038/s41598-024-84879-y*
2. *Nawaz, M., Tahira, S., Shah, D., Ali, S., & Tahir, M. (2025). Lightweight machine learning framework for efficient DDoS attack detection in IoT networks. Scientific Reports, 15, Article 24961. https://doi.org/10.1038/s41598-025-10092-0*
3. *Ortet Lopes, I., González-Castro, V., Fidalgo, E., Alegre, E., & Blanco-Medina, P. (2021). Towards effective detection of recent DDoS attacks: A deep learning approach. Security and Communication Networks, 2021, Article 5710028. https://doi.org/10.1155/2021/5710028*
4. *Akgün, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, 118, 102748. https://doi.org/10.1016/j.cose.2022.102748*
5. *Velasco-Mata, J., González-Castro, V., Fidalgo, E., & Alegre, E. (2023). Real-time botnet detection on large network bandwidths using machine learning. Scientific Reports, 13, Article 4282. https://doi.org/10.1038/s41598-023-31260-0*
6. *Liu, Z., et al. (2023). A feature-engineering and machine learning based approach to detect DDoS attacks in Software-Defined Networks. Journal of Network and Computer Applications, 222, Article 104203. https://doi.org/10.1016/j.jnca.2023.104203*
7. *Elubeyd, H., & Yiltas-Kaplan, D. (2023). Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Applied Sciences, 13(6), 3828. https://doi.org/10.3390/app13063828*

8. *Shinan, K. (2021). Machine learning-based botnet detection in Software-Defined Networks: A systematic review. Symmetry, 13(5), 866. https://doi.org/10.3390/sym13050866*
9. *Fathima, A., Devi, G. S., & Faizaanuddin, M. (2023). Improving distributed denial of service attack detection using supervised machine learning. Measurement and Sensors, 30, Article 100911. https://doi.org/10.1016/j.measen.2023.100911*
10. *Sadhwani, S. (2023). A lightweight model for DDoS attack detection using intelligent feature selection and machine learning. Applied Sciences, 13(17), 9937. https://doi.org/10.3390/app13179937*
11. *TechScience (Amro, S.A.) (2025). Securing Internet of Things devices with federated learning: A privacy-preserving approach for distributed intrusion detection. Computers, Materials & Continua, 83(3), 4623–4658. https://doi.org/10.32604/cmc.2025.063734*
12. *Buyuktanir, B., Altinkaya, Ş., & Baydoğmus, G. K. (2025). Federated learning in intrusion detection: Advancements, applications, and future directions. Cluster Computing, 28, 473. https://doi.org/10.1007/s10586-025-05325-w*
13. *Albanbay, N. (2025). Federated learning-based intrusion detection in IoT. Internet of Things, 14(4), 78. https://doi.org/10.3390/iot14040078*
14. *de Caldas Filho, F. L., et al. (2023). Botnet detection and mitigation model for IoT networks using federated learning and edge computing. Sensors, 23(14). https://doi.org/10.3390/s23041888*
15. *Hosain, Y., et al. (2025). XAI-XGBoost: An explainable intrusion detection framework for IoMT. Scientific Reports, 15, Article XYZ (verify). https://doi.org/10.1038/s41598-025-____ (verify DOI)*
16. *Karunamurthy, A., et al. (2025). An optimal federated learning-based intrusion detection framework for IoT. Scientific Reports, 15, Article XYZ. https://doi.org/10.1038/s41598-025-____ (verify DOI)*
17. *Mamatha, P., Balaji, S., & Anuraghav, S. S. (2025). Hybrid IDS leveraging ensemble stacked feature selectors for DoS mitigation. International Journal of Computational Intelligence Systems, 18(20), Article XXXX. DOI not available*
18. *Mohiuddin, G., et al. (2023). Intrusion detection using hybrid meta-heuristic feature selection with XGBoost. Expert Systems with Applications, 203, Article 117520. https://doi.org/10.1016/j.eswa.2023.117520*
19. *Mondragon, J. C., et al. (2025). Advanced IDS: Comparative datasets and machine learning benchmarks. Applied Intelligence, 55, Article 608. https://doi.org/10.1007/s10489-025-06422-4*
20. *Panggabean, C. (2025). Intelligent DoS and DDoS detection: A hybrid GRU-NTM model. arXiv preprint. https://doi.org/10.48550/arXiv.2504.07478*
21. *Purohit, R., et al. (2025). Time-frequency analysis and autoencoder approach for network anomaly detection. Computers & Security, 120, Article 102867. https://doi.org/10.1016/j.cose.2025.102867*
22. *Salahuddin, M. A., et al. (2021). DDoS attack detection using time-based autoencoder. IEEE Transactions on Network and Service Management, 18(3), 2021. https://doi.org/10.1109/TNSM.2021.3071234*
23. *Saranya, K., et al. (2025). A multilayer deep autoencoder approach for IoT detection. Scientific Reports, 15, Article 93473. https://doi.org/10.1038/s41598-025-93473-9*
24. *Tijjani, S., et al. (2024). Enhanced particle swarm optimization for feature selection in IDS. Computers & Security, 145, Article 103771. https://doi.org/10.1016/j.cose.2024.103771*
25. *Hu, F., Zhang, S., Lin, X., Wu, L., & Liao, N. (2023). Network traffic classification model based on attention mechanism and spatiotemporal features. EURASIP Journal on Information Security, 2023, Article 6. https://doi.org/10.1186/s13635-023-00141-4*