Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 13. Issue.2, PP. 89-95, December 2025
https://doi.org/10.22555/pjets.v13i2.1434
E-ISSN 2224-2333
P-ISSN 2222-9930

A Framework for Real-Time Continual Learning Federated Intrusion Detection Systems

Salahuddin Jokhio [1*], Asif Aziz Memon [2], Mahaveer Rathi [3], Zulfiqar Hussain Pathan [4], Ahmed Sikander [5]
[1]Department of Computer Science, University of Victoria, British Columbia, Canada.
[2,5] Department of Cyber Security, Dawood University of Engineering & Technology, Karachi
[3]Department of Computer Science, Government College University, Hyderabad
[4]Department of Data Science, Dawood University of Engineering & Technology, Karachi

[*]Corresponding Author: salahuddinjk@gmail.com

Abstract:

Intrusion Detection and Prevention Systems (IDS/IPS) are vital components of security architecture for protecting the networks against cyberattacks. Traditional IDS/IPS rely on static rules and user configurations, which make them less effective against growing threats. Modern studies have integrated Artificial Intelligence (AI) and Machine Learning (ML) into IDS to improve accuracy and detection speed. However, such AI/ML-based systems still face numerous issues, including reliance on outdated datasets, limited handling of zero-day attacks, a lack of interpretability, and privacy concerns. This paper studies recent AI/ML-based IDS/IPS works to identify key shortcomings and then proposes a real-time, continually learning, federated IDS framework with integrated explainable AI. The proposed framework design addresses the adaptability, privacy, and trustworthiness aspects, which can be used to build more resilient network defense systems.

Keywords: *Artificial intelligence, Intrusion Detection and Prevention Systems, Machine Learning, Security.*

I. INTRODUCTION

Network security is crucial for protecting systems from unauthorized access, exploitation, and disruptions. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are an integral part of any security infrastructure. IDS analyzes the network traffic and alerts security administrators about any suspicious activities, while IPS has an additional feature of automatically blocking or rejecting the malicious traffic. Early works in intrusion detection focused on signature-based and anomaly-based methods. Signature-based systems, such as Snort [4], match network patterns against known malicious signatures. Anomaly-based IDS/IPS, first modeled in [2][18][19], are used for detecting abnormal patterns from established behaviors.

Although these IDS/IPS systems have been widely deployed, they still suffer from many limitations. Static rules, manual feature design, and vulnerability to avoidance techniques reduce their effectiveness in modern communication networks. Several works, including surveys and classifications of these IDS methods, are available, such as [6], [7], [8], [13], which provide a detailed understanding of these traditional methods in a structured flow.

Due to the increasing complexity of these cyberattacks, there has been a recent interest in the development of Artificial Intelligence (AI) and Machine Learning (ML) based IDS/IPS. This adds automatic analysis and detection of malicious activities learnt from patterns, ultimately reducing the burden of continuous manual configurations. However, despite these state-of-the-art methods, existing AI/ML-based systems suffer from issues such as relying on outdated datasets, a lack of real-world validation, and privacy protection.

This paper provides a review of recent AI/ML-based IDS/IPS works, identifies major shortcomings, and then proposes a new real-time, federated, and explainable IDS framework to address these persistent challenges.

II. TRADITIONAL IDS/IPS SYSTEMS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are systems used to monitor network traffic and protect it from any malicious activity [16]. IDS detects suspicious activities within the network, while IPS can block them as well [14][15]. Traditional IDS/IPS systems are mainly categorized into two methods: signature-based and anomaly-based methods [17].

A. Signature-Based Systems

Signature-based systems detect attacks by comparing incoming data to a database of known attack patterns called signatures. Snort [4], a well-known signature-based system, has been highly deployed in practice. Such systems are highly effective at identifying and blocking known attacks. However, they fail to detect new or modified attacks unless a matching signature is configured into the system, and also struggle to detect cyber threats, which are increasing every day [20][21].

B. Anomaly-Based Systems

Anomaly-based systems detect attacks by identifying deviations from normal network behavior. An early anomaly-based system was introduced in [2]. These systems can detect unknown or novel attacks, but they often generate a high number of false alarms, as defining normal behavior precisely is quite a difficult task; also, with the help of ANOVA, they extract high-level features [22].

C. Key Limitations of Traditional IDS/IPS

Despite being the most common implementation of IDS/IPS, traditional systems have major drawbacks, which include static rules, manual feature design, and often suffer from evasion attacks.

Static Rules: The rules (signature databases) need frequent manual updates to be able to detect new or modified attacks.

Manual Feature Design: Defining useful detection features often requires expert knowledge and can be quite complex, due to the continuous evolution of attacks and changing tactics from malicious actors.

Evasion Attacks: Skilled attackers modify their behavior to bypass known detection techniques, hence evading manual configurations. The behaviour of an attack cannot be modeled into rules or features of an attack.

Due to aforementioned problems, there have been many studies exploring the integration of AI and ML in IDS/IPS to make the network more resilient to attacks, and IDS/IPS efficient and adaptive.

III. AI/ML IN INTRUSION DETECTION AND PREVENTION: RECENT ADVANCES

The use of AI/ML in intrusion detection and prevention is an active research area. These methods improve detection accuracy, adaptability, and automation. This section discusses various AI domains where ML has been applied to IDS/IPS.

A. Supervised Learning Techniques

Supervised learning models are trained using labeled datasets where the correct output is known, and models are expected to return the known labels. Classifiers such as Support Vector Machines (SVMs), Decision Trees (DTs), and Random Forests (RFs) are commonly used to detect malicious activities. Several works have studied supervised learning techniques for IDS. A framework based on feature selection and machine learning was proposed in [1]. This work aimed to enhance detection speed and efficiency. A work in [4] reviewed supervised methods for different types of intrusion, addressing the advantages of these methods. Another study in [12] provided a systematic review of supervised ML models used for network intrusion detection. Various techniques for feature selection in supervised IDS design were presented in [7].

Supervised models are seen to gain high accuracy on various commonly used datasets. However, it is still a challenge to deploy them in real-world environments where attack patterns constantly keep changing.

B. Deep Learning Based Systems

Deep Learning (DL) models learn complex patterns from data without manual feature engineering. IDS systems have been designed using Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, resulting in effective IDS Systems. Researchers in [10] discussed deep learning models for IDS, mainly CNNs and RNNs. Anomaly detection using DL techniques was discussed in [11], which studied their ability to detect unknown attacks. A meta-analysis on deep learning-based anomaly detection methods in network intrusion systems was carried out in [3].

Despite their handling of large datasets efficiently and improving generalization, DL models often require significant computational resources and large labeled datasets for training.

C. Federated and Privacy-Preserving Learning

Federated learning (FL), a decentralized machine learning approach, makes it possible for multiple clients to collaboratively train a model without sharing raw data. This is fundamental to IDS since network data can contain Personally Identifiable Information (PII) and sensitive information. [9] discussed federated learning methods applied to IDS. They studied issues such as communication overhead, data heterogeneity, and security risks from an FL perspective.

Federated IDS is good for preserving privacy and reducing the centralization risks. However, the design of an efficient federated learning model that can accurately detect attacks remains an open research problem.

D. Feature Selection and Dimensionality Reduction

Network traffic data is often multi-dimensional. Selecting the right features will improve the IDS efficiency and reduce false positives. The study in [7] addressed supervised feature selection techniques. Feature engineering challenges and dimensionality reduction methods were discussed in [5], where combining AI-based and traditional cybersecurity techniques was suggested for threat detection.

Feature selection reduces model complexity and enhances interpretability, but finding optimal features in constantly changing environments remains difficult, such as continuously changing network payloads.

IV. CRITICAL ANALYSIS OF EXISTING WORKS

There have been major advancements in the domain of AI/ML-based IDS/IPS. However, there are still many challenges that remain to be addressed. In this section, key achievements and major shortcomings are briefly discussed based on the latest works.

A. Key Achievements

Studies in [1], [4], [10], and [12] show that high accuracy for detection rate can be achieved on benchmark datasets. [3] and [11] prove that anomaly-based design and DL based models can also detect unknown and modified attacks better than conventional signature-based methods. Hence, not only do these enhanced AI systems automate the identification of threats, reducing the need for manual reviews, but they can speed up the network protection in real-time, as discussed in [1], [5].

B. Major Shortcomings

Most of the work in this domain mainly does performance evaluation of ML techniques on common datasets such as NSL KDSS and CICIDS 2017 [4], [12], which are outdated as they don't reflect evolving network traffic. In addition, very few works test their models in real-world networks. It should be noted that controlled datasets will always differ from real-world conditions, where the traffic is often unpredictable. Another aspect to consider is the training of the models, since ML-based models rely on data used in training [1], [12], hence ultimately not being able to detect novel threats and attacks without the need for retraining. Other things to consider are not being able to handle zero-day attacks, lack of interpretability (black box ML) on why a particular decision was made [10], and privacy issues with federated learning [9]. Table 1 provides a summary of such works, the datasets used in the work, the techniques utilized, and analyzes the strengths/weaknesses.

Table 1: Summary of AI/ML IDS/IPS Studies

Paper	Dataset Used	Main Technique	Strengths	Weaknesses
[1]	NSL KDD	Feature selection and ML	Fast, efficient	Limited to a single dataset
[3]	Multiple (CICIDS, NSL KDD, etc.)	Deep Learning	Anomaly detection	High resource needs
[4]	Mixed datasets	Survey	Broad coverage	Relies on older works
[5]	N/A	Combined AI and traditional methods	Practical integration	No experimental validation
[7]	KDD-99, NSL KDD	Feature selection	Complexity reduction	Not validated on new traffic
[9]	Simulated data	Federated Learning	Privacy preservation	Performance variation across nodes
[10]	CICIDS 2017	Deep learning (CNN, RNN)	Good for complex patterns	Poor explainability
[11]	N/A	Anomaly detection	Detects new threats	High false positives
[12]	CICIDS 2017	ML	Comprehensive benchmarking	Focused on academic settings

V. REAL-TIME CONTINUALLY LEARNING FEDERATED INTRUSION DETECTION FRAMEWORK

To address the limitations identified in current AI/ML-based IDS/IPS, we propose a Real-Time, Continually Learning, Federated Intrusion Detection Framework. The proposed architecture aims to enhance adaptability, privacy, and interpretability in AI-based IDS. The proposed framework has the following core components.

Dynamic Model Updates (Online Learning): Each participating node updates its local detection model continuously with newly arriving data, as opposed to retraining statically with new data, allowing the IDS to learn evolutionary attack vectors without needing an exclusive retraining.

Federated Aggregation to Preserve Privacy: The model updates (not the raw data) are sent periodically to a central aggregator by each node, which aggregates these updates into a global model. This reduces risks related to data exposure, maintains data privacy, and essentially computational load balancing and distribution.
Explainable AI (XAI) for Human-Readable Alerts: Each detection decision is given along with an explanation generated by a lightweight XAI module. This helps security analysts understand the detection decisions, i.e., the human-readable alerts, improve trustworthiness, and faster response actions from humans, if required. Figure 1 illustrates the conceptual architecture of the proposed framework.

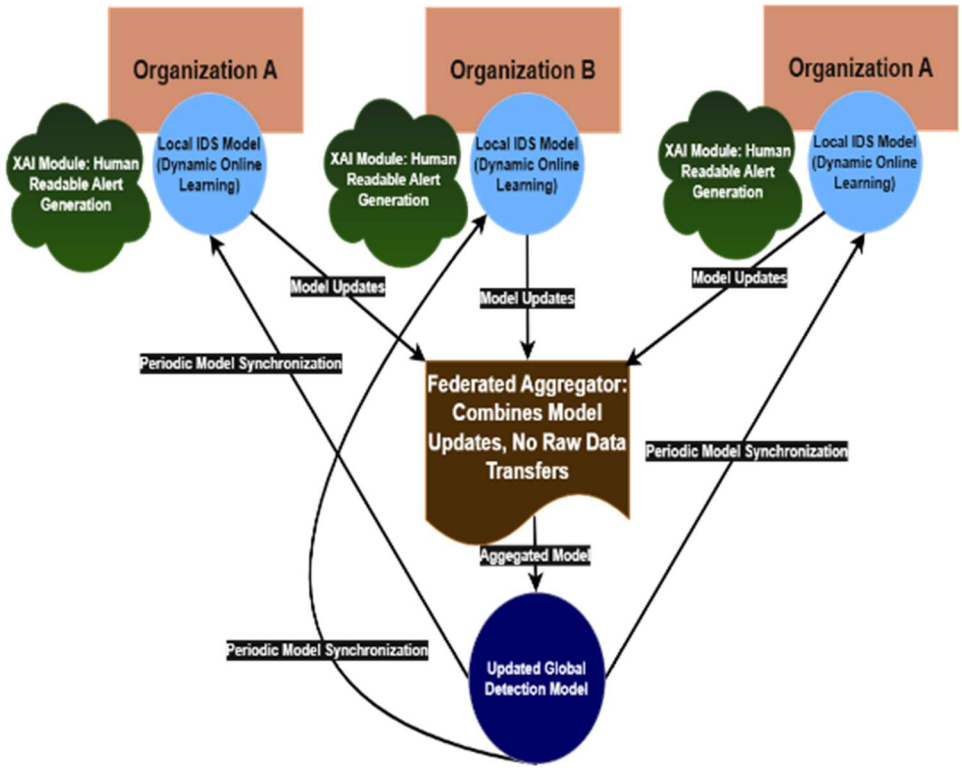

Figure 1. Proposed Real-Time Continually Learning Federated Intrusion Detection Framework

The proposed framework directly addresses several major limitations of current AI/ML-based IDS. By using continual online learning, the system continuously evolves with live network traffic rather than depending on outdated static datasets such as NSL KDD, CICIDS 2017, or others. This helps detect new threats without frequent manual retraining. The use of federated learning allows real-world deployments across multiple organizations while preserving the privacy of sensitive data, making practical validation feasible without exposing the raw network logs. These real-time updates

to each model and to the global model also enhance the security system's ability to recognize and respond to zero-day attacks with higher probability, which often go undetected by static models trained on existing datasets. To address the interpretability problem commonly seen in black box models, each decision made by the system is paired with a human-readable explanation generated by a lightweight XAI module. This increases human analysts' trust and helps in a faster incident response. Finally, because federated learning combines model updates instead of raw data, the framework reduces the data centralization risks and protects network confidentiality by a wide margin.

VI. CONCLUSION

Intrusion detection and prevention remain two important areas of information security in general. Traditional IDS/IPS systems, while effective against known threats, face several major challenges such as limited adaptability, almost no zero-day detection, and risk related to data privacy. Recent advances in AI and ML have improved detection accuracy and reduced response times. However, most of the existing solutions still rely mainly on common static datasets, with almost no real-world deployment validation, and they suffer from models' decision interpretability issues.

This work first reviewed and introduced recent IDS/IPS works inspired by AI/ML and identified the main loopholes that need urgent attention. To address these gaps, we proposed a real-time, continually learning, federated intrusion detection framework. This design combines online learning, federated model aggregation, and an integrated explainable AI component to build adaptive systems, privacy-preserving and human-trustworthy.

As far as future work is concerned, implementing and evaluating such architectures under live network environments would be an interesting direction. As the implementation would continuously monitor the network and system activities in real time for the system's unwanted behavior, it would be helpful for the system to take timely action on such activities and mitigate the security risks. Furthermore, the policy and documentation can be configured for organization standards, and regular tuning and maintenance would be scheduled to optimize the detection performance. Long-term deployment studies will also be quite important towards understanding the operational strengths and limitations of dynamic, federated, and interpretable IDS models.

REFERENCES

[1] G. P. Gupta and M. Kulariya, "A framework for fast and efficient cyber security network intrusion detection using Apache Spark," *Procedia Computer Science*, vol. 93, pp. 824–831, 2016.
[2] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, no. 2, pp. 222–232, 1987.
[3] Z. K. Maseer, Q. K. Kadhim, B. Al-Bander, R. Yusof, and A. Saif, "Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges," *IET Networks*, vol. 13, no. 5–6, pp. 339–376, 2024.
[4] M. Roesch *et al*., "Snort: Lightweight intrusion detection for networks," in *Proc. 13th USENIX Conf. System Administration (LISA)*, Seattle, WA, USA, 1999, pp. 229–238.
[5] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning-based network intrusion detection," *Electronics*, vol. 8, no. 3, p. 322, 2019.
[6] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using Bayes estimators," in *Proc. SIAM Int. Conf. Data Mining (SDM)*, 2001, pp. 1–17.
[7] M. Di Mauro, G. Galatro, G. Fortino, and A. Liotta, "Supervised feature selection techniques in network intrusion detection: A critical review," *Engineering Applications of Artificial Intelligence*, vol. 101, p. 104216, 2021.
[8] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Tech. Rep. 99-15, Dept. Comput. Eng., Chalmers Univ. Technol., 2000.
[9] S. Agrawal *et al*., "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Computer Communications*, vol. 195, pp. 346–361, 2022.
[10] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," *Processes*, vol. 9, no. 5, p. 834, 2021.
[11] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2009.

[12] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly-based intrusion detection systems using the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021.
[13] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Boston, MA, USA: Pearson, 2021.
[14] M. Sheeraz, M. H. Durad, S. Tahir, H. Tahir, S. Saeed, and A. M. Almuhaideb, "Advancing Snort IPS to achieve line-rate traffic processing for effective network security monitoring," *IEEE Access*, vol. 12, pp. 61848–61859, 2024.
[15] T. Vaiyapuri *et al*., "Metaheuristics with federated learning-enabled intrusion detection system in Internet of Things environment," *Expert Systems*, vol. 40, no. 5, e13138, 2023.
[16] Q. Xu, L. Zhang, D. Ou, and W. Yu, "Secure intrusion detection by differentially private federated learning for inter-vehicle networks," *Transportation Research Record*, vol. 2677, no. 3, pp. 591–603, 2023.
[17] S. H. Hajj *et al*., "Cross-layer federated learning for lightweight IoT intrusion detection systems," *Sensors*, vol. 23, no. 16, p. 7038, 2023.
[18] R. Zhao *et al*., "A federated learning approach to network intrusion detection using residual networks in industrial IoT networks," *The Journal of Supercomputing*, vol. 80, pp. 18325–18346, 2024.
[19] S. H. Hajj *et al*., "A heterogeneity-aware semi-decentralized model for a lightweight intrusion detection system for IoT networks based on federated learning and BiLSTM," *Sensors*, vol. 25, no. 4, p. 1039, 2025.
[20] K. R. Ahmed *et al*., "Enhancing signature-based intrusion detection system for IoT networks using machine learning algorithms," in *Proc. Int. Conf. Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*, IEEE, 2025.
[21] U. Ahmed *et al*., "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports*, vol. 15, no. 1, p. 1726, 2025.
[22] M. Arafah *et al*., "Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks," *Applied Soft Computing*, vol. 168, p. 112455, 2025.