A Privacy-Preserving Hybrid Intrusion Detection System for IoT Networks Using Federated and Deep Learning Models

Shrishti Kumari
Department of CSE
Technocrats Institute of Technology (Excellence), Bhopal, Madhya Pradesh, India
shrishtikumari1511@gmail.com

Sugandh Singh
Department of CSE
Technocrats Institute of Technology (Excellence) Bhopal, Madhya Pradesh, India

Arjun Rajput
Department of CSE
Technocrats Institute of Technology (Excellence) Bhopal, Madhya Pradesh, India

Surbhi Karsoliya
Department of CSE,
Technocrats Institute of Technology
Bhopal, Madhya Pradesh, India

Abstract: The exponential increase in IoT devices has truly brought in security challenges never noticed before from heterogeneous traffic patterns with limited resources and f]rom ever-changing cybercriminal behaviors. This study proposes a privacy-preserving Intrusion Detection System (IDS) for IoT environments through the integration of FL with sophisticated DL models. The framework utilizes AE, DNN, and a hybrid AE+CNN architecture for anomaly detection and intrusion classification. Model evaluation was conducted using N-BaIoT, a dataset comprising traffic from different IoT devices under genuine attack scenarios. Data preprocessing steps such as normalization, encoding, and feature engineering were carried out to improve data quality and reduce noise. The FL paradigm allows distributed training on IoT devices without any exposure of raw data to any intermediary, thereby strengthening privacy and scaling. Experimental results show that AE obtains an accuracy of 95% and strong anomaly-detection abilities, whereas FL+DNN attains an accuracy of 90.39% and higher precision (97.99%) for classifying known attacks. The hybrid AE+CNN bettered all other models with 96.5% accuracy maintained a balance on recall and precision and showed great robustness toward zero-day and complex attacks. Comparative analysis reveals that the more light-weight nature of AE+CNN makes it suitable for edge and defense against imbalance more, while FL+DNN is better suited to privacy-aware distributed settings. This study exemplifies how unsupervised and supervised DL techniques under FL offer a powerful potential to develop efficient, scalable, and accurate IDS solutions. Future work will try to direct false positives reduction, explainable AI, and feasibility enhancement to deployments on real-world IoT systems.

Keywords: Intrusion Detection System, IoT Security, Federated Learning, Autoencoder, Deep Neural Network, Convolutional Neural Network, Hybrid Deep Learning.

I. INTRODUCTION

Increasing dependence on interconnected systems continues to make organizations vulnerable to highly sophisticated cyber threats, underscoring the urgent need for more-evolved security provisions to keep pace. Keeping the records of network activities, the IDS may detect any anomalies and warn the administrator against potential intrusion attempts [1]. While firewalls directly block unauthorized access, IDSs analyze network traffic continuously and accrue information that can be useful to detect the traces of malicious activity in its early stages along before the developers are able to mount attack fronts. The role of an IDS has grown from simple pattern matching to developing an intelligent computational system that can discover hidden intent behind patterns in the network data set; the data are enormous and high dimensional [2]. These acts will continue to extenuate the need for ID systems. Early attacks were limited to simple viruses or worms, while DDoS (Distributed Denial of Service), advanced persistent threats (APT), zero-day exploits, and ransomware are the tools of today's adversary [3]. The more these IoT devices appear, and cloud-based systems continue to grow in acceptance, so does their various attack vectors. Plus, attackers actually use AI (Artificial Intelligence) and ML (Machine Learning) to hide from detections, thus marking methods by conventional IDS obsolete. This implies that the IDSs must be adaptive and intelligent, learning from the dynamic environment and catching both known and unknown threats [4].

Traditional IDS approaches, each based on a signature, anomaly, or specification, present their own pros and cons. Signature-based IDSs detect known attacks with perfect accuracy, but they fail to protect against zero-day attacks and need to be updated continuously [5]. Anomaly-based IDSs, on the other hand, detect novel attacks by flagging deviations from what is deemed normal behavior. These systems may, however, cause dirt-level false positives, drowning security analysts with alerts, many of them unnecessary. Specification-based IDSs look for the rules that correspond to a predefined notion of expected system behavior. Nonetheless, they tend to be resource-heavy and difficult to deploy at scale in a large heterogeneous network. Collectively, all these drawbacks portray conventional IDS methods as inadequate in tackling today's ever-changing and complicated cybersecurity landscape [6]. Machine learning is increasingly being seen as an aid in boosting IDS efficacy. Supervised algorithms, such as

Received 2 June 2025, Accepted 23 August 2025

decision trees, random forests, and Support Vector Machines (SVM), are best at discriminating between given attack types, whereas unsupervised techniques like clustering and SOMs address new forms of attacks. Semi-supervised learning attempts to compensate for data scarcity by utilizing a combination of limited labeled data and masses of unlabeled traffic [7]. Feature engineering assumes a key role in ML-enabled IDS, seeing that network traffic usually comes in the form of high-dimensional attributes, many of which can be redundant. Techniques to prune down attribute space and compare relevance may include recursive feature elimination, chi-square testing, and dimensionality reduction, making tasks efficient for the detection facility and saving computational power. On their merits, however, ML systems have an issue generalizing across never-seen-before malware and falsely classify some traffic because of overlapping traffic traces, whereas in certain class imbalance cases, they produce a fairly large number of false positives. Figure 1. illustrates the Intrusion Detection System.

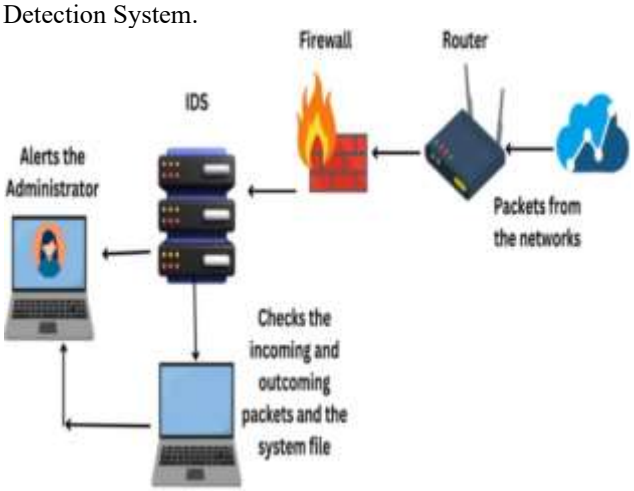

Figure 1 Intrusion Detection System [2]

In further advancing IDS design, DL learns the hierarchical features directly from raw network traffic. Architectures of CNN would capture the spatial correlations, while RNN and LSTM models would capture the temporal dependencies [8]. Autoencoders are used in anomaly detection; they reconstruct normal traffic behaviors to detect deviations as intrusions. Hybrid models coupling 2 or more DL architectures have been promising in detecting both simple and very complex attacks. The wearable scalability and the ability to operate in massive high-dimensional data environments make DL very apt for cyber-security applications in real-time [9]. However, its need for a large set of labeled samples, the high computation costs, and its lack of interpretability give rise to major challenges. Given the complementary strengths and weaknesses of ML and DL, hybrid frameworks have gained promising consideration in IDS research. While ML lends interpretability, efficiency, and low computational demand, DL brings in automated extraction of features, better precision, and adaptability to ever-changing threats. These two under which together can build an intelligent and resilient IDS that handles imbalanced data, detects zero-day attacks, and scales to large, heterogeneous environments [10].

The above advancements cannot cease. However, the very key challenges remain there. We must balance IDSs between detection accuracy and false alarms with real-time scalability and resolve model transparency performance issues so that an analyst can reasonably interpret the decisions made by the models [11]. Imbalance in datasets and quickly changing attack strategies make it increasingly difficult to put the classifier into effective training and deployment. A solution to all of these challenges lies in certain innovative approaches that allow the flexible adaptability of DL at times; at others, it allows the efficiency of ML and builds in a layer for explainability and resource efficiency [12]. Promoted by the urgent need of having a hybrid ML-DL IDS architecture to negate the limitations of individual models, this study intends to develop an IDS achieving high detection accuracy, robustness against novel attacks, and scalability in real-time scenarios. It aims to engineer such an IDS by mixing supervised and unsupervised model designs, feature engineering, and advanced deep learning architectures. For the applicability of the system, it would be tested on benchmark datasets that contain various traffic and attack signatures. The final goal is to fill the gap existing between theoretical advancements in IDS research and their operational deployment, thereby aiding in developing stronger adaptive cyber-defenses which can thus be trusted.

II. RELATED WORK

While recent years have seen growing and growing interest in attack detection systems via machine learning and deep learning, researchers keep applying optimized techniques to improve accuracy, robustness, and adaptability. The hybrid machine learning framework studied the integration of preprocessing, feature selection, and ensemble supervised learners, yielding a balance between accuracy, precision, recall, and F1-scores. However, the system was primarily dependent on some handcrafted selection of features in the training phase, limiting the scalability of the approach in practical scenarios [13]. Taking it a step further, this deep learning method combined Extra Trees for feature selection with a CNN–RNN hybrid classifier, thus reporting binary classification accuracy of 97.93%, while precision, recall, and F1 scored 97% as well. On the other hand, robustness with respect to adversarial drift remained unknown [14].

Another more interesting paradigm is Federated Learning, whereby local models get adapted with some sort of secure aggregation. Such schemes reported approximately 92 percent accuracy and 82 percent F1, but the issue of non-IID data with poisoned clients always posed challenges related to communication overhead and trust [15]. Likewise, an IDS for vehicular ad hoc networks adopted a bidirectionally sparse attention recurrent autoencoder whose recall was excellent for novel attacks, yet scalability to large high throughputs was still problematic [16].

Taking IoT security into account, a smart deep learning model comprising an XGBoost optimized for feature selection with deep classifiers attained outstanding performance, even yielding 99.93% accuracy on NSL-KDD, 99.84% F1, and a false positive rate of 0.0004. Yet, its dependence on older benchmarks was seen as a

drawback, leading to overfitting and failure to reflect the diversity of modern attacks [17]. Besides this, an LSTM, coupled with cosine similarity, managed to beat other models in terms of accuracy, precision, recall, and F1 on UNSW and BoT-IoT datasets, but this setup remained sensitive to sequence windowing and data imbalance [18].

Industrial IoT environments motivated hybrid schemes deploying CNNs with attention in federated settings, yielding improved accuracy and privacy preservation with respect to centralized baselines but added model complexity and communication burden [19]. Reinforcement learning approaches also entered the domain-the Deep Q-Learning intrusion detection system reported an accuracy of 97.09% and an F1-score of 98.52%, although limitations such as instability in training as well as interpretability prevented its widespread deployment [20].

Frameworks for evaluation have been proposed with the aim of systematic benchmarking of models for IDS, showing many of the previously reported gains to shrink under the cross-dataset-standardized conditions. It is then that the standardization set in, showing how fragile certain results based on the choice of the dataset or on the scheme of preprocessing can become [21]. Other novel structures, such as HSO-ResNet, presented in the context of seagull metaheuristics for optimization, achieve high levels of accuracy and recall in testbeds where a massive amount of data was fed, but their heavy computational load makes them unrealistic for deployment in edge or real-time environments [22].

On alternative representations, network traffic is imaged and classified with LeNet-style CNNs, attaining accuracies nearing 90% on the NSL-KDD and sometimes beyond, a good measure of merit. Still, the image-based representations were considered sensitive to the encoding selections and selection of artifacts [23]. Ensemble approaches such as stacking through subspace clustering have reported 97.05% accuracy, 96.33% precision, 96.55% recall, and 96.45% F1, but were criticized for using outdated datasets and added inference costs [24].

Federated learning surveys established that these methods could maintain their initial high performance in accuracy, precision, recall, and AUC metrics alongside the improvement of privacy. However, their reliance on synthetical or IID data splits exposed their vulnerability to real-world heterogeneity [25]. Autoencoders, CNNs, and RNNs were compared for novelty detection and classification. The results demonstrated that AEs and hybrid methods work best for novelty detection, whereas CNNs are best for known signatures. Metrics reported include perfect precision, recall, F1, and ROC-AUC; however, the results varied widely with the choice of preprocessing method [26]. Finally, an advanced IIoT framework is reported to provide 97.8% accuracy on the X-IIoTID dataset with stable AUC per class but its generalization potential to other environments and the interpretability of deep features remain open questions [27].

Table 1 Machine Learning and Deep Learning Techniques for IDS

Ref	Technique Used	Dataset(s) Used	Results	Limitations
[13]	Preprocessing + feature selection + ensemble supervised learners	NSL-KDD, CICIDS2017	High accuracy, balanced precision, recall, and F1	Relies on handcrafted feature selection; limited real-world validation
[14]	Extra Trees + CNN/RNN hybrid	CICIDS2017	Accuracy 97.93%, Precision 97%, Recall 97%, F1 97%	Evaluated only on curated dataset; robustness to adversarial drift untested
[15]	Federated learning with secure aggregation	UNSW-NB15, BoT-IoT	Accuracy ~92%, F1 ~82%	Degrades with non-IID data and poisoned clients; communication overhead
[16]	Bi-directional sparse-attention recurrent autoencoder (VANET IDS)	VANET traffic dataset	High recall for novel attacks; better than baseline AEs	Specialized to VANET; scalability and latency issues
[17]	XGBoost + deep classifiers (IoT IDS)	NSL-KDD	Accuracy 99.93%, F1 99.84%, FPR 0.0004	Uses older benchmark; risk of overfitting; limited to outdated attacks
[18]	LSTM with cosine similarity	UNSW-NB15, BoT-IoT	Outperformed other models in accuracy, precision, recall, F1	Requires tuning of sequence windows; class imbalance issues
[19]	CNN + attention in federated learning (IIoT)	IIoT traffic datasets	Improved accuracy and privacy vs centralized models	Model complexity, communication overhead; limited adversarial testing
[20]	Deep Q-learning IDS (DQN-style RL)	CICIDS2017	Accuracy 97.09%, F1 98.52%	Training instability; long training episodes; poor interpretability
[21]	Evaluation framework for ML-based IDS	CICIDS2017, NSL-KDD, UNSW-NB15	Showed inflated metrics shrink under standardized, cross-dataset evaluation	Results depend heavily on dataset/preprocessing choices

[22]	ResNet-101 optimized with seagull metaheuristic (HSO-ResNet)	UNSW-NB15	High accuracy and recall reported	High computational burden; impractical for edge deployment
[23]	LeNet-style CNN with traffic-to-image encoding	NSL-KDD, CICIDS2017	Accuracy ~90% (NSL-KDD), near-100% in setups	Encoding introduces artifacts; results sensitive to preprocessing
[24]	Stacking ensemble with subspace clustering	UNSW-NB15	Accuracy 97.05%, Precision 96.33%, Recall 96.55%, F1 96.45%	Uses outdated datasets; ensemble increases inference complexity
[25]	Federated learning survey & evaluation	UNSW-NB15, CICIDS2017	Maintained accuracy, precision, recall, AUC vs centralized	Relies on IID splits; vulnerable to non-IID and poisoning
[26]	Comparative study: Autoencoder, CNN, RNN	NSL-KDD, CICIDS2017	Reported strong precision, recall, F1, ROC-AUC; AEs excel in novelty detection	Results vary with preprocessing; no universally best model
[27]	Deep IDS framework (X-IIoTID dataset)	X-IIoTID (IIoT-specific dataset)	Accuracy 97.8%, str	

III. RESEARCH OBJECTIVES

- To develop a privacy-preserving IDS for IoT using Federated Learning.
- To integrate Autoencoder, DNN, and CNN for intrusion detection.
- Use the N-BaIoT dataset for realistic model evaluation.
- Apply pre-processing and feature engineering to improve data quality.
- To evaluate models with accuracy, precision, recall, and F1-score.

IV. RESEARCH METHODOLOGY

The methodology developed a privacy-preserving IDS for the IoT. The approach covers federated learning with sophisticated deep learning models for the detection of both known and zero-day attacks while overcoming issues of data privacy, heterogeneity, and resource constraints across IoT devices.

a. Overall Framework

Conventional IDSs work on a model of centralized data collection and training. They, however, present shortcomings with respect to privacy, scalability, and single points of failure. To avoid this, an FL paradigm is promoted by the proposed IDS that allows IoT devices to train global models in a collaborative manner without sharing raw traffic data. Each device receives the global model, trains it locally on traffic data, shares the weights to a central server, and model updates are aggregated using Federated Averaging with Momentum (FedAvgM), hence preserving privacy and scalability. The framework combines the following three core deep learning models. The AE method is a potential technique for the detection of anomalies via unsupervised learning through minimizing reconstruction error suitable for zero-day attacks.Deep Neural Network (DNN) model, for supervised classification of labeled traffic, that captures nonlinear patterns in network data.An AE + CNN-in-the-loop model, where the AE serves as a feature extractor, whereas the CNN captures spatial and hierarchical features from traffic, improving classification accuracy and generalization performance.

b. Dataset

The N-BaIoT dataset was utilized, containing over 7 million records and 115 features generated from nine commercial IoT devices, including cameras, thermostats, and smart plugs. Traffic encompasses benign behavior and malicious patterns generated by Mirai and BASHLITE botnets. The attacks are in 10 categories ranging from DDoS, UDP flooding, scanning, to combo attacks, together with the benign traffic. Though comprehensive and realistic, the imbalance within the dataset is severe with benign samples greatly outnumbering malicious samples; hence careful pre-processing is necessary.

c. Data Pre-processing

A set of actions for pre-processing was established to increase data quality: Data Cleaning: Removal of duplicate records, corrupted records, and treating missing values through imputation. Transformation: Normalization and scaling of features to ensure uniform range. Encoding: One-hot encoding and label encoding of categorical attributes. Feature Engineering: Dimensionality reduction, feature selection, and derivation of statistics for exposing hidden attack patterns. This makes sure that the models had balanced input that was free from noise and computationally inexpensive. Figure: 2 Architecture of AE model.

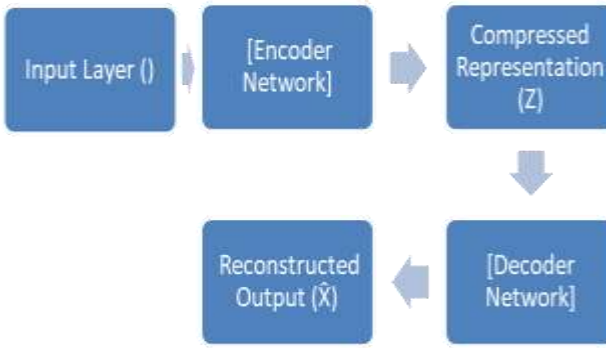

Figure 2 Architecture of AE model

d. Model Development

Autoencoder (AE): Built with encoder–decoder architecture and trained to reconstruct benign traffic. Any traffic with a high reconstruction error is flagged as an anomalous event. DNN (with FL): Consisting of multiple fully connected layers with ReLU activation and dropout regularization, it uses several optimizers such as Adam, SGD, and RMSProp. Each client trains the model locally, while the updates are aggregated by FedAvgM.AE +CNN Hybrid: AE first compresses the raw features into latent representations, which are then passed to CNN with convolution, pooling, and fully connected layers for classification. This hybrid enhances the detection of more subtle and zero-day threats. Figure 3 presents Systematic diagram of CNN model

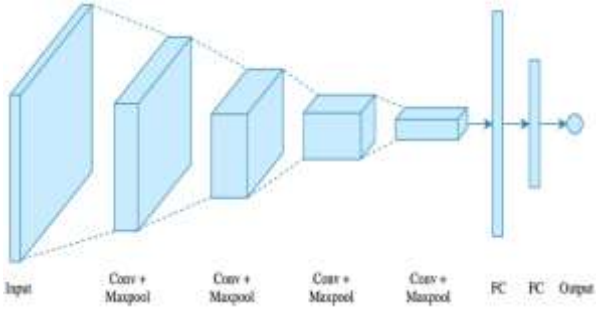

Figure: 3 Systematic diagram of CNN model

e. Evaluation Metrics

Following evaluation procedures were executed to map performance along: Accuracy, Precision, Recall, F1-score, True Positive Rate, False Positive Rate, and even the AUC-ROC or Area Under the Curve. These metrics pump fairness into evaluation and are even more so crucial with imbalanced datasets such as N-BaIoT.

$$\text{Accuracy:}\frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{PRECISION:}\frac{TP}{TP+FP} \quad (2)$$

$$\text{RECALL:}\frac{TP}{TP+FN} \quad (3)$$

$$\text{F1: } 2\times\frac{Precision\times Recall}{Prcision+Recall} \quad (4)$$

V. RESULT AND DISCUSSION

VI. CONCLUSION AND FUTURE WORK

This study demonstrates the combination of federated learning with deep learning architectures to constitute an efficient, privacy-preserving solution for intrusion detection in IoT networks. With this, the presence of Autoencoders for unsupervised anomaly detection, Deep Neural Networks for supervised classification, and a hybrid AE+CNN model for feature extraction and attack recognition would make the proposed IDS able to tackle the problems of heterogeneous IoT traffic, resource constraints, and evolving attack patterns. Experimental evaluations were performed on the N-BaIoT dataset, revealing that the AE attained 95% accuracy with good anomaly detection capability, the FL+DNN model detected known attacks with a precision of 97.99%, whereas AE+CNN hybrid obtained the best results with 96.5% accuracy and well-balanced recall and precision. The results show that while FL+DNN suits distributed privacy-preserving environments, AE+CNN remains light and edge-deployable and is perhaps the best solution for known and zero-day attack detections. More attention will be given in the future to developing methods to reduce false positives and further improve detection accuracy on imbalanced IoT datasets. Explainable AI could be employed to improve interpretability, thus creating more trust in the decisions of the IDS. Another area of focus would be on real-world large-scale deployment and integration with existing network-monitoring frameworks.

Conflict of Interest: The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.

References

[1] S. Jones, "Machine learning-based intrusion detection framework for detecting security attacks in Internet of Things," *Scientific Reports*, vol. 14, no. 1, p. 81535, Dec. 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-81535-3.

[2] S. Jones, "Network-based intrusion detection using deep learning technique," *Scientific Reports*, vol. 15, no. 1, p. 8770, Aug. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-08770-0.

[3] G. K. Baydogmus, Ş. Altinkaya, and K. Yildiz, "Federated learning in intrusion detection:

advancements, applications, and future directions," *Cluster Computing*, vol. 28, p. 473, Aug. 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10586-025-05325-w.

[4] R. Gopi, V. T. Kesavan, and J. Hossen, "Bi-directional sparse attention recurrent autoencoder based intrusion detection system in VANET," *Scientific Reports*, vol. 15, no. 1, p. 2729, Aug. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-02729-x.

[5] F. S. Alsubaei, "Smart deep learning model for enhanced IoT intrusion detection," *Scientific Reports*, vol. 15, no. 1, p. 20577, Jul. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-06363-5.

[6] A. Prasad, W. M. Alenazy, N. Ahmad, G. Ali, H. A. Abdallah, and S. Ahmad, "Optimizing IoT intrusion detection with cosine similarity based dataset balancing and hybrid deep learning," *Scientific Reports*, vol. 15, no. 1, p. 30939, Aug. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-15631-3.

[7] J. Huang, Z. Chen, S.-Z. Liu, H. Zhang, and H.-X. Long, "Improved intrusion detection based on hybrid deep learning models and federated learning," *Sensors*, vol. 24, no. 12, p. 4002, Jun. 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/12/4002.

[8] Md. A. Hossain, "Deep Q-learning intrusion detection system (DQ-IDS): A novel reinforcement learning approach for adaptive and self-learning cybersecurity," *ICT Express*, vol. 11, no. 1, pp. 181–188, May 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959525000694.

[9] S. Jones, "Evaluating machine learning-based intrusion detection systems with performance metrics," *Frontiers in Computer Science*, vol. 7, p. 1, Aug. 2025. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2025.00001/full.

[10] S. Jones, "Intrusion detection: A comparison study of machine learning algorithms," *SN Computer Science*, vol. 5, no. 1, p. 1, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s42979-024-01000-0.

[11] S. Jones, "Intrusion detection in IoT and wireless networks using image-based techniques," *ScienceDirect*, vol. 11, no. 1, pp. 1–10, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864825000450.

[12] S. Jones, "A multiclass network intrusion detection system using stacking classifiers," *Journal of Applied and Intelligent Technologies*, vol. 2, no. 1, p. 1, 2025. [Online]. Available: https://jait.org/articles/10.1007/s42452-025-1089-4/.

[13] V. Kantharaju, H. Suresh, M. Niranjanamurthy, S. Immamul Ansarullah, F. Amin, and A. Alabrah, "Machine learning based intrusion detection framework for detecting security attacks in Internet of Things," *Scientific Reports*, vol. 14, no. 1, p. 81535, Dec. 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-81535-3.

[14] Farhan, M., Waheed Ud Din, H., Ullah, S., Hussain, M. S., Khan, M. A., Mazhar, T., ... & Jaghdam, I. H. (2025). Network-based intrusion detection using deep learning technique. *Scientific Reports*, *15*(1), 25550.

[15] B. Buyuktanir, Ş. Altinkaya, and K. Yildiz, "Federated learning in intrusion detection: advancements, applications, and future directions," *Cluster Computing*, vol. 28, p. 473, Aug. 2025. [Online]. Available: https://link.springer.com/article/10.1007/s10586-025-05325-w.

[16] Gopi, R., Thiruppathy Kesavan, V., Jakir Hossen, M., & Abdul Aziz, N. H. B. (2025). Bi directional sparse attention recurrent autoencoder based intrusion detection for VANET security with tuna swarm optimization. Scientific Reports, 15(1), 18406..

[17] F. S. Alsubaei, "Smart deep learning model for enhanced IoT intrusion detection," *Scientific Reports*, vol. 15, no. 1, p. 20577, Jul. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-06363-5.

[18] A. Prasad, W. M. Alenazy, N. Ahmad, G. Ali, H. A. Abdallah, and S. Ahmad, "Optimizing IoT intrusion detection with cosine similarity based dataset balancing and hybrid deep learning," *Scientific Reports*, vol. 15, no. 1, p. 30939, Aug. 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-15631-3.

[19] J. Huang, Z. Chen, S.-Z. Liu, H. Zhang, and H.-X. Long, "Improved intrusion detection based on hybrid deep learning models and federated learning," *Sensors*, vol. 24, no. 12, p. 4002, Jun. 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/12/4002.

[20] Md. A. Hossain, "Deep Q-learning intrusion detection system (DQ-IDS): A novel reinforcement learning approach for adaptive and self-learning cybersecurity," *ICT Express*, vol. 11, no. 1, pp. 181–188, May 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959525000694.

[21] Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, *111*(4), 2287-2310.

[22] Ajagbe, S. A., Awotunde, J. B., & Florez, H. (2024). Intrusion detection: A comparison study of machine learning models using unbalanced dataset. *SN Computer Science*, *5*(8), 1028.

[23] Sun, Y., & Wang, Z. (2025). Intrusion detection in IoT and wireless networks using image-based neural network classification. *Applied Soft Computing*, 113236.

[24] Tang, Y., Gu, L., & Wang, L. (2021). Deep stacking network for intrusion detection. *Sensors*, *22*(1), 25.
[25] Deshmukh, A., de la Rosa, P. E., Rodriguez, R. V., & Dasari, S. (2025). Enhancing Privacy in IoT-Enabled Digital Infrastructure: Evaluating Federated Learning for Intrusion and Fraud Detection. *Sensors*, *25*(10), 3043.