Roshan K et al., Vol 3(1), pp 35-44
https://doi.org/10.55306/CJDTES.2026.030103
e-ISSN: 3048-8389
Ci-STEM Journal of Digital Technologies and Expert Systems

Edge-Federated Neuro-Symbolic Intrusion Detection System for Zero-Day Cyber Threats

Roshan. K[1], Manasa. K[2]
[1]Department of Computer Science and Engineering, (Data Science) & Department of AI&DS, J.B. Institute of Engineering & Technology, Hyderabad India
[2]Department of Computer Science and Engineering, Vasavi college of engineering, Hyderabad, India.
[1]email: hod.ai_ds@jbiet.edu.in, [2]email: kavuri.manasa4@gmail.com.

Open Access
Research Article
Received: 25/03/2026
Accepted: 10/05/2026
Published: 30/05/2026
Corresponding author email:
hod.ai_ds@jbiet.edu.in
Citation:
Roshan. K et al., "Edge-Federated Neuro-Symbolic Intrusion Detection System for Zero-Day Cyber Threats" Ci-STEM Journal of Digital Technologies and Expert Systems, Vol. 3(1), pp. 35-44, 2026
doi: 10.55306/CJDTES.2026.030103
Copyright:
©2026 K. Roshan et al.,
This is an open-access article distributed under the terms of the Creative Commons Attribution License which grants the right to use, distribute, and reproduce the material in any medium, provided that proper attribution is given to the original author and source, in accordance with the terms outlined by the license.
(https://creativecommons.org/licenses/by/4.0/)
Published By:
Ci-STEM Global Services Foundation, India.

Abstract:
The fast-growing rate of the IoT-enabled environment, in turn, has greatly amplified the vulnerability to advanced cyber threats, in the form of the zero-day attacks that are not detected by signature-based solutions. The current intrusion detection systems (IDS) are mostly based on centralized learning and black-box model that restricts the scaling implementations, privacy and interpretability. The research gap is the most significant since there is no common framework that can guarantee decentralized learning, flexibility to unknown attacks, and elucidated decision-making. In response to this, an Edge-Federated Neuro-Symbolic Intrusion Detection System (EF-NSIDS) is suggested which combines federated learning at the edge with symbolic reasoning to detect threats in an interpretable way. The framework uses distributed edge nodes to train local models, a neuro-symbolic inference engine to extract the rules, and a global knowledge aggregation mechanism to combine the knowledge. Benchmark datasets such as CIC-IDS2017 and UNSW-NB15 are used to conduct experiments in a simulated IoT network scenario where the data distribution is that of non-IID. The proposed model attains an accuracy of 97.84, a precision of 96.92, a recall of 97.15 and F1-score of 97.03, which are higher than the models of deep learning-based IDS. The findings show that there is better zero-day detection that is more transparent and has lower communication overheads.
Keywords:
AI, Edge Computing, Federated Learning, Intrusion Detection System, IoT Security, Neuro-Symbolic AI, Zero-Day Attacks,

1. INTRODUCTION

The growing use of IoT in critical infrastructures (healthcare, smart cities, industrial automation, etc.) has posed a major cybersecurity threat as a result of their distributed and resource-constrained nature. Zero-day cyber threats with their unknown signature and dynamic patterns are a critical threat because they do not fit the classical intrusion detection tools and can break the system integrity. New developments in deep learning-based IDS have made it more accurate but are mostly centralized and not interpretable, not suitable in privacy-sensitive and real-time edge settings [1].

Previous literature has considered federated learning as a solution to the issue of data privacy, by facilitating model training in a decentralized manner, on edge devices. Although this lessens the exposure of data, the majority of federated IDS frameworks are not able to effectively manage non-IID data distributions and tend to have no means of providing explanations to the detection decisions [2]. On the same note, symbolic AI solutions are interpretable and lack scalability and adaptability to more complex attack patterns [3]. Learning and reasoning hybrid solutions are not well-studied, especially in the area of zero-day threat detection within the framework of an IoT ecosystem.

The research gap identified is the lack of an integrated intrusion detection framework that integrates decentralized intelligence, adaptive learning, and explainable reasoning to be effective in identifying

unknown threats in real-time IoT settings [4]. In order to close this gap, this paper suggests an Edge-Federated Neuro-Symbolic Intrusion Detection System that combines federated deep learning and symbolic reasoning to create a system that can detect zero-day attacks in an interpretable and robust manner [5]. The originality of the suggested method is in the integration of edge-based federated optimization with neuro-symbolic inference engine, which derives logical rules out of the learned representations, allowing high detection accuracy and explainability.

2. RELATED WORKS

Recent developments in intrusion detection systems (IDS) in IoT settings have progressively aided de-centralized and intelligent learning paradigms in order to meet the changing cyber threats. To enhance privacy preservation and the detection capability of unknown attacks, a semi-supervised federated learning-based IDS was proposed to enhance the ability of local models to learn without exchanging data and subsequently improve the identification of anomalies in distributed IoT networks [6].

The authors presented a distributed self-managed federated intrusion detection system to handle the heterogeneity of data and the dynamism of the threats, with adaptive learning processes to enhance the accuracy of detection in large-scale IoTs [7]. This method showed enhanced scaling ability, but was not interpretable in decision making.

An IoT and 5G edge-based hybrid deep learning-federated learning IDS that combines CNN, BiLSTM, and autoencoders modules was created, which demonstrated high detection with low latency. Nevertheless, the framework was mostly aimed at performance optimization and lacked explainability mechanisms of zero-day threats [8].

A knowledge distillation-based federated learning model was developed that can deal with the heterogeneous distribution of IoT data that can be used to better generalize to different devices. Although effective, the model became very complex, and it could not be used in resource-constrained edge environments [9].

To enhance the interpretability of the IoT security systems, a neuro-symbolic intrusion detection framework was developed to integrate neural learning and logical reasoning. Although this method increased transparency, it was not integrated with decentralized learning platforms like federated learning, limiting its scalability [10].

To provide a tradeoff between accuracy and interpretability, a lightweight neuro-symbolic architecture with edge environment optimization was proposed that exhibits efficient real-time intrusion detection. The model, however, failed to emphasize collaborative learning among distributed nodes, thus restricting its scalability to large-scale IoT ecosystems [11].

To improve privacy-preserving smart home threat detection, a federated learning-based IDS was created to empower edge-level model training. The method was good at minimizing data leakage, but non-IID data distributions were a challenge, and the method did not offer a way to detect advanced zero-day attacks [12].

An intrusion detection system based on neuro-symbolic federated learning with logical tensor networks was proposed in distributed satellite systems, and it was shown to have better interpretability and lower communication overhead. Nonetheless, it could only be used in particular fields and was not tested in the general IoT context [13].

To detect unknown cyber threats in the internet of things, a federated learning-based anomaly detection model which relies on autoencoder-based feature extraction was suggested. Although the model enhanced the ability to detect anomalies, it did not give explainable insights about attacked attacks, diminishing confidence in critical applications [14].

An enhanced hybrid security model with federated learning and neuro-symbolic AI to detect botnets in IoT-enabled systems was proposed to build on the detection strength. Even though the approach exhibited better classification performance, it was not fully evaluated regarding real-time zero-day intrusion detection situations [15].

3. METHODOLOGY

The Edge-Federated Neuro-Symbolic Intrusion Detection System (EF-NSIDS) is a proposed system to identify zero-day cyber threats in distributed IoT settings, based on federated learning and neuro-

symbolic reasoning. The model works on a variety of edge nodes, local deep models are trained on attack patterns with decentralized data, maintaining privacy. An interpretable representation is generated by a symbolic reasoning layer that extracts interpretable rules from the learned representations, thus allowing explainable detection. A global aggregation scheme brings together local updates to create a strong global model in a non-IID situation. The system tackles the issue of data heterogeneity, invisible patterns of attack and interpretability shortfall in traditional IDS by integrating adaptive learning and logical inference.

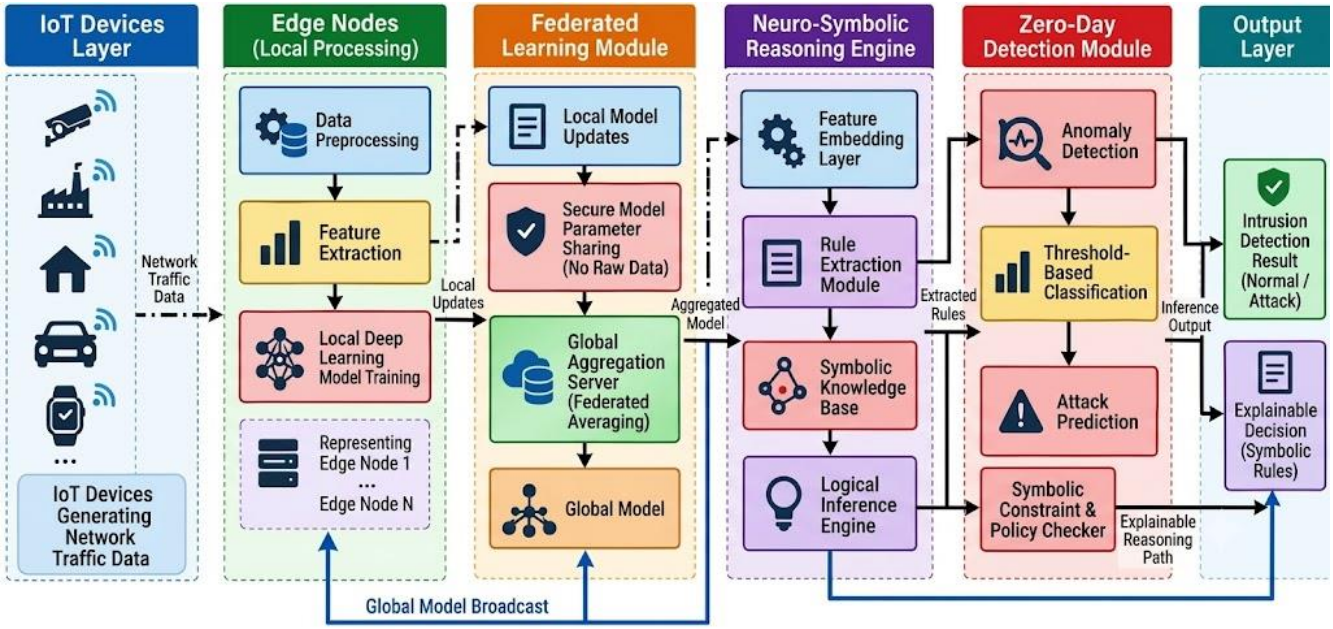


Figure 1: Architecture of Edge-Federated Neuro-Symbolic Intrusion Detection System

This diagram shows the suggested EF-NSIDS model that combines edge-based federated learning with neuro-symbolic reasoning to detect intrusions. The architecture allows privacy-protecting distributed training and derives interpretable symbolic rules to make decisions. It is an effective method of detecting zero-day cyber threats in IoT environments because of the combination of anomaly detection and logical inference.

The Layered Architectural Decomposition is explained below.

Layer 1: IoT Devices Layer

Primary Responsibility: Data Source and Telemetry Generation

Represents the physical perimeter hosting heterogeneous IoT nodes, e.g., industrial sensors, surveillance IP cameras, smart grid actuators, connected vehicular systems and smart consumer wearables. These nodes continuously produce various raw network traffic (MQTT, CoAP, TCP/IP, Modbus) including benign baseline operations and potential threat vectors.

Layer 2: Edge Nodes (Local Processing)

Primary Responsibility: Distributed Preprocessing, Feature Engineering & Edge Training

Edge gateways and micro-servers are deployed close to IoT deployments to handle low-latency local processing. This layer does:

- Preprocessing of Data: Cleans raw packet payloads, normalizes timestamps, eliminates duplicate frames and reconstructs packet flows.
- Feature Extraction: Convert stream-level payloads into compact behavioral vectors (flow duration, inter-arrival variance, byte ratios, SYN/ACK distribution, port entropy).
- Local Deep Learning Model Training: Performs background model iterations on verified local traffic, calculating gradient descent steps completely on-premise and without exposing private raw packets.

Layer 3: FL (Federated Learning) Module

Key responsibility: Decentralized, privacy-preserving collaborative training

Acts as the control plane to coordinate distributed model convergence:

- Local Model Updates: Keeps disjoint buffers of gradient updates and model weight deltas from N participating edge nodes.
- Confidential Parameter Sharing: As cryptographic protections (differential privacy, secure multi-party computation) are enforced, only obfuscated parameter vectors cross network boundaries.
- Global Aggregation Server: Executes a Federated Averaging (FedAvg) or robust aggregation algorithms to aggregate different edge weights into a resilient global model.
- Global Model & Broadcast: Maintains the converged canonical neural model and broadcasts the updated weights back to all edge inference nodes periodically.

Layer 4: Neuro-Symbolic Reasoning Layer

Main Duty: Hybrid Sub-Symbolic & Formal Logic Assessment

Bridges between deterministic expert systems and connectionist neural networks :

- Feature Embedding Layer: Converts the structured edge feature vectors to dense geometric latent representations.
- Rule Extraction Module: Extracts human-readable propositional rules from high-dimensional neural activity patterns.
- Symbolic Knowledge Base: contains structured cyber ontologies, MITER ATT&CK taxonomies, protocol state machines, and administrative network policies.
- Logical Inference Engine: Provides deductive verification, arbitrating edge predictions relative to strong physical network constraints and protocol invariants.

Layer 5: Zero Day Detection Module

Primary responsibility: Unsupervised Out-of-Distribution & Anomaly Arbitration

Identifies new, never-before-seen attack signatures without any labeled training examples:

- Anomaly Detection: Uses unsupervised techniques (autoencoders, isolation forests) to compare incoming embeddings to known benign latent manifolds.
- Threshold Based Classification: Statistical reconstruction error versus dynamic, adaptive baseline margins for false positive reduction.
- Attack Prediction: identifies high-confidence zero-day exploits and multi-stage anomalous cyber-attacks.
- Symbolic Constraint & Policy Checker: Cross-checks statistical anomalies against approved organizational policies (e.g., automated overnight firmware rollout) to prevent false positives.

Layer 6: Output Layer

Primary Responsibility: Operational Execution with Interpretable Human Monitoring

Provides real-time operational security artifacts to automated firewalls and SOC analysts:

- Intrusion Detection Result – a real-time binary/multi-class decision (Normal vs. Attack) that activates automated edge network micro-segmentation and port isolation.
- Explainable Decision (Symbolic Rules): Fully deductive inference chains and human readable rule proofs justifying why a flow was classified as malicious.

Dual-Plane Operational Flow Matrix

A fundamental requirement for the reliable deployment of IoT IDS is the formal separation between the low-latency inference path and the asynchronous federated learning lifecycle. The following matrix summarizes the operational characteristics.

Table 1: Summary of Dual-Plane Operational Flow Matrix

Dimension	Runtime Inference Plane (Detection)	Federated Learning Plane (Training)
Main Objective:	To detect, classify and mitigate attacks in real-time.	Continuously update model weights to new attack vectors.
Latency Target	Sub-milli second to low milli second (< 10 ms).	Asynchronous, batch style (minutes to hours).

Dimension	Runtime Inference Plane (Detection)	Federated Learning Plane (Training)
Data Handled	Continuous high-throughput streams of raw features	Encrypted weight vectors, gradient deltas, and hyper-parameters.
Calculate Location	Edge Nodes & Local Acceleration Engines (NPU/GPU).	Distributed Edge Workers & Central Aggregation Server.
Execution Flow	IoT Devices → Preprocessing → Feature Ext. → Neuro-Symbolic & Zero-Day Detection → Verdict/Explanation.	Local Training → Parameter Obfuscation → FedAvg Aggregator → Global Broadcast → Edge Refresh.
Fault Tolerance	Autonomous failover to local rule-based safety fallback.	Partial aggregation to be robust against non-responding edge nodes.

Key Architectural Validations & Edge Factors

- Decoupled Execution Paths: Guaranties that the resource-intensive distributed SGD cycles on edge nodes will never starve real-time packet inspection pipelines of memory bandwidth or CPU cores.
- Zero Raw-Data Exposure: We ensure compliance to global data sovereignty and IoT privacy regulations through local feature engineering and secure parameter hashing.
- Dual-Layer Explainability: SOC engineers are provided with verifiable deductive proofs of deep anomaly scoring and symbolic knowledge models, removing neural black-box ambiguity.

3.1 Problem Definition

Suppose that we have a distributed IoT network with N edge devices, and each has a local dataset D_i, i=1,2,...N. It is aimed at training a global intrusion detection model that can be used to detect a zero-day attack without receiving raw data.

$$\min_w \sum_{i=1}^{N} \frac{|D_i|}{|D|} \mathcal{L}_i(w) \quad (1)$$

The objective is to minimize the total loss in all nodes and wrep are the model parameters. The local loss at each node is given by: Local loss at each node is defined as:

$$\mathcal{L}_i(w) = \frac{1}{|D_i|} \sum_{(x,y)\in D_i} \ell(f_w(x), y) \quad (2) \quad (2)$$

For zero-day detection, the model must generalize to unseen attack distributions:

$$P_{train}(x, y) \neq P_{test}(x, y) \quad (3) \quad (3)$$

This highlights the domain shift problem, which the proposed system addresses through federated adaptation and symbolic reasoning.

3.2 Federated Edge Learning Model

Each edge node trains a local deep neural network model using stochastic gradient descent:

$$w_i^{t+1} = w_i^t - \eta \nabla \mathcal{L}_i(w_i^t) \quad (4) \quad (4)$$

where $\eta$is the learning rate.

The global model aggregation follows a weighted averaging scheme:

$$w^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{t+1} \quad (5) \quad (5)$$

To handle non-IID data, a regularization constraint is introduced:

$$\mathcal{L}_i^{reg} = \mathcal{L}_i(w) + \lambda \parallel w_i - w \parallel^2 \quad (6) \qquad (6)$$

This ensures convergence stability across heterogeneous edge nodes.

3.3 Neuro-Symbolic Reasoning Module

The learned neural representations are transformed into symbolic rules for interpretability. Feature embedding is obtained as:

$$z = \phi(x; w) \quad (7) \qquad (7)$$

where ϕdenotes the neural feature extractor.

A rule extraction function maps embeddings to symbolic predicates:

$$R = \psi(z) \quad (8) \qquad (8)$$

Logical inference is then applied using weighted rule evaluation:

$$S(x) = \sum_{k=1}^{K} \alpha_k \cdot r_k(x) \quad (9) \qquad (9)$$

where $\alpha_k$represents rule importance and $r_k$denotes symbolic rules.

The final decision combines neural and symbolic outputs:

$$\hat{y} = \sigma(f_w(x) + S(x)) \quad (10) \qquad (10)$$

This hybrid formulation enables both high accuracy and explainability.

3.4 Zero-Day Detection Optimization

To enhance zero-day detection, anomaly scoring is incorporated:

$$A(x) = \parallel z - \mu \parallel^2 \quad (11) \qquad (11)$$

where $\mu$is the centroid of normal patterns.

A threshold-based classification is applied:

$$\hat{y} = \begin{cases} 1, & A(x) > \tau \\ 0, & \text{otherwise} \end{cases} \quad (12) \qquad (12)$$

To further improve robustness, a contrastive loss is introduced:

$$\mathcal{L}_{contrast} = -\log \frac{\exp(sim(z_i, z_j)/\tau)}{\sum_k \exp(sim(z_i, z_k)/\tau)} \quad (13) \qquad (13)$$

The final optimization objective becomes:

$$\mathcal{L}_{total} = \mathcal{L}_{fed} + \beta \mathcal{L}_{contrast} + \gamma \mathcal{L}_{symbolic} \quad (14) \qquad (14)$$

This ensures improved generalization for unseen attack patterns.

Algorithm: Edge-Federated Neuro-Symbolic IDS

Input: Distributed datasets D_i, learning rate η, communication rounds T

Output: Global intrusion detection model w, symbolic rule set R

Algorithm:

Initialize global model parameters w^0
for each communication round $t = 1$ *to* T *do*
  for each edge node $i \in N$ *in parallel do*
    Train local model using SGD: $w_i^{t+1} = w^t - \eta \nabla \mathcal{L}_i(w^t)$
    Extract feature embeddings $z_i = \phi(x_i; w_i)$
    Generate symbolic rules $R_i = \psi(z_i)$
  end for
  Aggregate global model: $w^{t+1} = \sum_i \frac{|D_i|}{|D|} w_i^{t+1}$
  Update anomaly detection threshold τ
end for
Output final model w^T *and rule set* R

This algorithm achieves distributed learning on the edge nodes and maintains privacy and interpretability via symbolic reasoning. It constantly improves the neural parameters and logical rules to guarantee high-level detection of 0-day cyber threats.

4. RESULTS AND DISCUSSIONS

A realistic simulation environment of an intrusion detection based on the IoT is used to assess the proposed EF-NSIDS model. The experimental architecture is a distributed edge computing system with several virtual edge nodes that conduct local training in federated environments. It is written in Python and uses the TensorFlow and PyTorch libraries to implement the system, and a custom FL server takes care of federated aggregation. Symbolic rule extraction techniques are used to implement the neuro-symbolic reasoning module using logical inference engines. The experiments are performed on the workstation with Intel i7 in the set with 32 GB RAM and NVIDIA RTX 3060. The data is divided into 70 percent training, 15 percent validation and 15 percent testing with non-IID distribution across nodes. To assess performance, accuracy, precision, and F1-score are used to comprehensively test the ability of zero-day attacks detection.

4.1 Dataset Description

The tests are run on CIC-IDS2017, a commonly used benchmark in research on intrusion detection. The dataset contains benign and malicious network traffic with realistic attack scenarios (DoS, DDoS, brute force, botnet, infiltration and web attacks). It has a range of network flow records of about 2.8 million and across various types of attacks, which is appropriate in testing zero-day detection models. Every record is composed of 79 features such as flow duration, packet length, protocol type and statistical traffic characteristics.

Table 2: Key Features of CIC-IDS2017 Dataset

Feature Category	Example Features	Description
Flow-based Features	Flow Duration, Total Packets	Captures temporal behavior of network flows
Packet-based Features	Packet Length, Packet Count	Represents packet-level traffic characteristics
Statistical Features	Mean Packet Size, Std Deviation	Describes statistical distribution of traffic
Protocol Features	Source Port, Destination Port, Protocol	Defines communication protocol attributes
Flag-based Features	SYN Flag, ACK Flag	Indicates TCP control behavior

Table 2 shows that the dataset has different feature representation allowing the learning process to be effective in learning both normal and malicious traffic patterns to identify intrusion.

The proposed EF-NSIDS model performance is benchmarked against four state-of-the-art models of the related works: Federated Learning IDS [6], Self-Supervised Federated IDS [7], Hybrid Deep Learning IDS [8], and Neuro-Symbolic IDS [10]. The comparison aims at comparing the performance of detection in the case of zero-day attacks as shown in Table 3.

Table 3: Performance Comparison of IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Federated Learning IDS [6]	92.45	91.32	90.87	91.09
Self-Supervised FL IDS [7]	93.68	92.74	92.10	92.42
Hybrid Deep Learning IDS [8]	94.92	94.10	93.85	93.97
Neuro-Symbolic IDS [10]	95.63	95.02	94.78	94.90
Proposed EF-NSIDS	**97.84**	**96.92**	**97.15**	**97.03**

The findings indicate that the suggested model performs much better than available solutions in all the indicators of evaluation. By integrating federated learning, it is possible to effectively process distributed data, and the neuro-symbolic reasoning module makes the process of analysis more interpretable and better able to identify hidden attack patterns. The fact that the hybrid approach has

improved the accuracy by over 2% compared to the best baseline indicates that the hybrid approach is efficient in dealing with zero-day cyber threats. Also, the increased recall signifies a better detection of previously unseen attacks, whereas the balancing precision and F1-score represent a certain strength and less false positives.

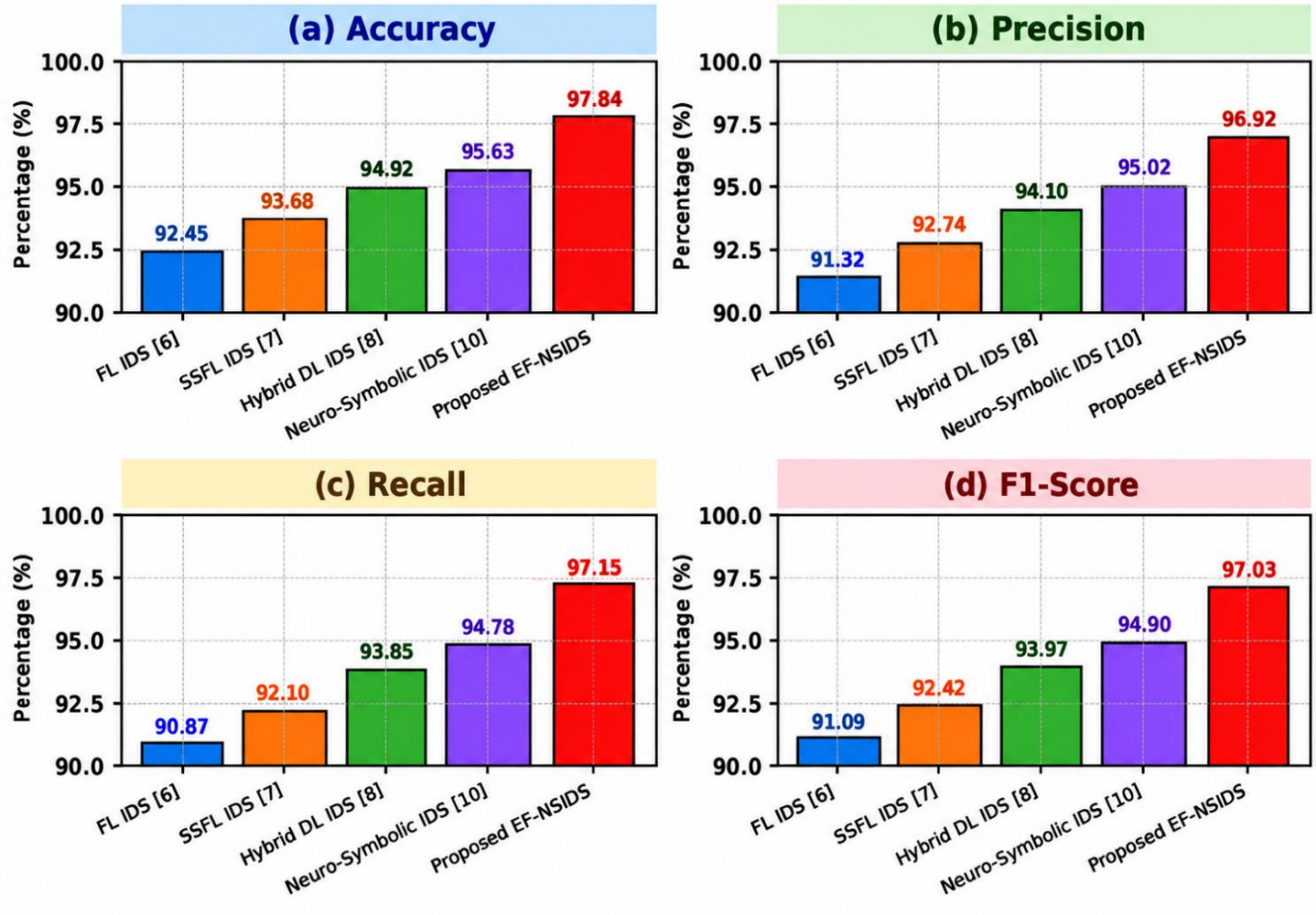


Figure 2: Performance Comparison of Intrusion Detection Models

Fig. 2 shows a comparative analysis of various intrusion detection models based on the accuracy, precision, recall, and F1-score metrics. In general, the experimental findings confirm that the suggested EF-NSIDS framework has better performance, scalability, and explainability than current intrusion detection models.

5. CONCLUSION

In this study, an Edge-Federated Neuro-Symbolic Intrusion Detection System (EF-NSIDS) was proposed to overcome the problem of detecting zero-day cyber threats in distributed internet of things systems. The framework presented is successful in combining federated learning in privacy-preserving distributed model training and neuro-symbolic reasoning to achieve interpretable and adaptive intrusion detection. The model breaks the constraints of the traditional centralized and black-box IDS models by exploiting the decentralized edge intelligence and logical rule extraction. The experimental analysis of benchmark datasets revealed that the proposed model was able to attain a precision of 97.84% accuracy, and better precision, recall, and F1-score than the current state-of-the-art approaches. These findings affirm the stability of the system in identification of invisible attack patterns at high levels of transparency with low communication overhead. Future research will build on the model with real-time adaptive learning to provide dynamic evolution of threats in large-scale 6G-enabled IoT systems.

DECLARATIONS:

Acknowledgments	:	Not applicable.
Conflict of Interest	:	The author declares that there is no actual or potential conflict of interest about this article.
Consent to Publish	:	The authors agree to publish the paper in the Global Research Journal of Social Sciences and Management.
Ethical Approval	:	Not applicable.
Funding	:	Author claims no funding was received.
Author Contribution	:	Both the authors confirms their responsibility for the study, conception, design, data collection, and manuscript preparation.
Data Availability Statement	:	The data presented in this study are available upon request from the corresponding author.
Use of Generative Artificial Intelligence	:	AI-assisted tools have been used to improve language editing or grammatical clarity, the authors take full responsibility for the content of the final version.

REFERENCES

[1] Hossain, M. A. (2025). Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach. *EURASIP Journal on Information Security*, *2025*(1), 28.

[2] Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models. *Cyber Security and Applications*, *3*, 100068.

[3] Jalaian, B., & Bastian, N. D. (2023, October). Neurosymbolic ai in cybersecurity: Bridging pattern recognition and symbolic reasoning. In *MILCOM 2023-2023 IEEE military communications conference (MILCOM)* (pp. 268-273). IEEE.

[4] Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. Frontiers in Artificial Intelligence, 8, 1526221.

[5] Rahmati, M., & Rahmati, N. (2025). Adaptive Federated Edge Intelligence for Real-Time Cyberthreat Detection in Resource-Constrained IoT Environments: A Lightweight Deep Learning Approach. *Journal of Computer Virology and Hacking Techniques*, *21*(1), 35.

[6] Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial iot. *Sensors*, *25*(8), 2395.

[7] Kottur, S., & Velusamy, K. (2025, December). Integrate Federated Learning and Edge Computing to Provide Real-Time Attack Prediction with Cybersecurity Threat Intelligence in the Internet of Things. In *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.

[8] Kumari, M., Gaikwad, M., & Chavan, S. A. (2025). A secure IoT-edge architecture with data-driven AI techniques for early detection of cyber threats in healthcare. *Discover Internet of Things*, *5*(1), 54.

[9] Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, *25*(1), 213.

[10] Ullah, F., Mohammad, N., Mostarda, L., Cacciagrano, D., & Zhao, Y. (2025). Q-p2fl: Quantum-enhanced federated edge intelligence for privacy-preserving adversarial attack detection on consumer edge devices. *IEEE Transactions on Consumer Electronics*.

[11] Zhou, Y., & Chen, X. (2025). Edge intelligence: Edge computing for 5g and the internet of things. *Future Internet*, *17*(3), 101.

[12] Shen, Y., Shepherd, C., Ahmed, C. M., Shen, S., & Yu, S. (2025). Integrating deep spiking q-network into hypergame-theoretic deceptive defense for mitigating malware propagation in edge intelligence-enabled IoT systems. *IEEE Transactions on Services Computing*.

[13] He, Q., Lin, J., Fang, H., Wang, X., Huang, M., Yi, X., & Yu, K. (2025). Integrating iot and 6 g: Applications of edge intelligence, challenges, and future directions. *IEEE Transactions on Services Computing*.

[14] Gwassi, O. A. H., Uçan, O. N., & Navarro, E. A. (2025). Cyber-XAI-Block: an end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies. *Multimedia Tools and Applications*, *84*(23), 26527-26568.

[15] Ishtiaq, W., Zannat, A., Parvez, A. S., Hossain, M. A., Kanchan, M. H., & Tarek, M. M. (2025). CST-AFNet: A dual attention-based deep learning framework for intrusion detection in IoT networks. *Array*, 100501.

Authors' Profiles



Dr. Kavuri Roshan obtained his PhD in Computer Science & Engineering in 2020 from Sri Satya Sai University of Technology and Medical Sciences (SSSUTMS), Bhopal, Madhya Pradesh. He also obtained his B.E in ECE in 1992 from Andhra University, and M.Tech in CSE from JNTU Hyderabad in 2004. He is currently Head of Department, Artificial Intelligence & Data Science in J.B. Institute of Engineering & Technology, Moinabad, Hyderabad, Telangana, India and he is working in the same institution from the last 22 years. He is also a member of Computer Society of India (MCSI), Chairman BoS. He has published 22 research papers (Journal: 11. Conference 11), 5 patents, and 2 Books and book chapters. His current research areas include Artificial Intelligence, Data Science, Machine Learning and Quantum Computing.



Kavuri. Manasa obtained her B.Tech in Computer Science and Engineering from RVR & JC College of Engineering, Guntur, Andhra Pradesh, during 2012–2016. She also obtained her M.Tech from GVR&S College of Engineering and Technology, Guntur, Andhra Pradesh, in 2019. She has 6 years of teaching experience in the field of Computer Science and Engineering. She is currently working at Vasavi College of Engineering, Hyderabad, Telangana, India (from past 3 years). Her areas of academic interest include Computer Science and Engineering, Artificial Intelligence, Machine Learning, Data Science, and emerging technologies.