INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

Cognitive Zero-Trust Networks Using Federated Threat Learning

Jyotsna Pandit[1] and Preeti Kumari[2]
[1]*Professor, Manav Rachna University, Faridabad, Haryana, India.*
[2]*Assistant Professor, Department of CSE & Apex, Chandigarh Engineering College, CGC Jhajeri, Mohali-140307, Punjab, India.*
[1]jyotsnapandit4@gmail.com, [2]preetikp7@gmail.com

Abstract. The dynamism and proliferation of IoT, edge, and cyber physical systems has brought complexity to contemporary networks as well as brought them close to extremely dynamic and dynamic cyber threats. Conventional intrusion detection infrastructure, as well as ancient Zero-Trust architecture, cannot work in those heterogeneous settings because it relies on centrally stored data, fixed trust analysis, and low flexibility in countering the zero-day assaults. To overcome those issues, Cognitive Zero-Trust Network based on Federated Threat Learning (C-ZTN-FTL), a smart, privacy-obliging framework, is proposed in this paper, which combines federated learning, cognitive trust calculation, and multi-layer fusion of threat knowledge. The model is proposed, which also has a Federated Threat Learning mechanism that combines encrypted gradients and latent threat embeddings so that the representation of the threat can be richer and generalize better across non-IID data environments. A Cognitive Trust Engine based on reinforcement-learning constantly updates the trust scores on the basis of local anomaly patterns, global threat settings, device posture, and history, providing context-based and dynamic Zero-Trust access control. The reasoning over unknown or new attack patterns is also improved further by multi-layer threat intelligence fusion at the level of IoT, edge, and cloud levels. As shown by the experimental findings based on the CIC-IDS-2017, UNSW-NB15, and IoTID20 datasets, the proposed system has a detection accuracy of 97.2, indicates a significant enhancement of the zero-day attack detection, a lower false-positive rate, more stable trust scoring by 18.3, and a reduction in the communication overhead by 35% relative to the baseline FL-IDS models. On the whole, the C-ZTN-FTL framework offers dynamic, scalable, and resilient solution to secure the contemporary distributed networks against high-level cyber threats.

Keywords: Cognitive Zero-Trust Architecture, Federated Threat Learning, Intrusion Detection System, IoT Security, Cyber Threat Intelligence, Reinforcement Learning, Zero-Day Attack Detection, Trust Computation.

1. Introduction

The recent explosion of Internet of Things (IoT) and edge devices as well as cyber-physical systems has greatly increased the contemporary attack surface, presenting networks with an ever-growing number of more complex and distributed cyber threats. The conventional intrusion detection systems are very much based on data gathering that is centralized and rules that are not dynamic and thus tend to pose privacy threats in addition to failing to respond to the heterogeneous and dynamic environments. With the growing use of sophisticated evasion methods, the use of the zero-day attacks, and the multi-vector attack, the shortcomings of the traditional security structure become even more evident. Zero-Trust Architecture (ZTA), founded on the idea of always verifying and never trusting, has become an excellent prospect regarding curbing the lateral movement and imposing continuous authentication. But the majority of the current ZTA deployments are based on a one-time trust measurement and are unintelligent to adapt to changing threat patterns or even auto-adjust policy in response to real-time changes.

Volume: 04 Issue: 04 Year: 2025
Received: 18.09.2025 Received in revised from: 09.10.2025 Accepted: 15.11.2025
Available Online: 29.12.2025
Published by NTL Publisher

Concomitant to this, another promising method is Federated Learning (FL) which is a privacy-protective intrusion detection method that trains a model and does not require raw data to be shared (centrally) with sensitive data. A number of studies have shown the possibility of FL-based IDS in enhancing the generalization and preserving privacy in distributed IoT devices. Nonetheless, the current FL-IDS solutions have three critical shortcomings: they are mainly passing gradient updates and cannot capture more profound behavioral attributes of attacks, prone to non-IID data distributions that deteriorate model convergence and accuracy, and do not incorporate cognitive reasoning or dynamic trust calculation, which is an inappropriate solution to Zero-Trust systems that require ongoing access decisions.

In order to fill these gaps, the present research presents a Cognitive Zero-Trust Network (C-ZTN-FTL) consisting of federal learning, cognitive trust computation, and multi-layered threat intelligence fusion, into a single security architecture. The suggested system uses the latent threat embeddings, global threat knowledge graphs and trust scoring through reinforcement-learning to make intelligent and adaptive security decisions. In contrast to conventional FL systems, Federated Threat Learning mechanism collects encrypted gradient updates in addition to latent threat signatures, enhancing the capacity of a system to identify a zero-day and hitherto unseen intrusions. Also, the Cognitive Trust Engine is continuously updating trust values and access rights according to anomaly reports in the real-time in addition to global threat associations and historical device history to then actively revise the policy in a Zero-Trust framework.

The major contributions that this work makes are:

1) a new Federated Threat Learning architecture that better represents the threat and detects it under non-homogenous data scenarios;
2) a cognition trust computation framework entirely based on reinforcement learning to dynamically tune device trustworthiness;
3) a zero-trust multi-layer architecture that incorporates device, edge, and cloud intelligence to mitigate any attack; and
4) comprehensive experimental analyses suffering ample improvements in accuracy, trust stability, zero-day detection as well as communication efficiencies.

On the whole, this work offers a scalable, privacy-sensitive, and intelligent Zero-Trust solution that can protect the current IoT and edge ecosystem against the ever-changing cyber-threats.

2. Literature Review

The recent booming IoT, edge, and cyber-physical systems have raised the necessity of privacy-sensitive, dynamic, and intelligence-led systems of intrusion detectors. The conventional centralized methods of intrusion detection can be classified as privacy violation, lack of scalability and potential failure at single points. Federated learning (FL) has become a potential solution to such difficulties and a promising paradigm that allows distributed model training without the exchange of raw data.

2.1 Federated Learning for Intrusion Detection

The initial study on FL-based intrusion detection showed high possibilities of enhancing privacy at an accuracy level. One of the initial FL-enabled wireless edge network intrusion detection systems was suggested in [4], which emphasizes the inability to decrease communication cost as well as the confidentiality of user data. Based on this kind of work, DeepFed was proposed in [3], a deep federated learning model on cyber–physical systems with significant enhancement in detection accuracy in more complex industrial traffic.

Further applications of FL extended FL to various IoT and edge applications. FL was used to detect malware in IoT devices in [5], where the authors showed that distributed learning has the capacity to boost resilience in heterogeneous environments. Likewise, the performance of FL on various IDS datasets was assessed in [6], where it was found that common problems such as non-IID data distribution and inconsistent model convergence remain. A detailed review in [7] further highlighted poisoning attacks, resource limitations, and challenges in deploying FL in dynamic network settings.

Later studies discussed architectures and threat scenarios. The evolution of FL-based IDS was reviewed in [8], emphasizing the need for lightweight architectures and secure aggregation mechanisms. A federated cyber threat intelligence sharing architecture was proposed in [9], which consolidated network-level attack information across distributed nodes. A complete FL pipeline for background IoT IDS was presented in [10], addressing feature heterogeneity and computational power constraints.

More recent works incorporated FL into automotive, fog, and heterogeneous IoT systems. A comprehensive taxonomy of FL-IDS for Internet of Vehicles (IoV) was proposed in [11], while an optimized FL framework to improve IDS training efficiency was introduced in [12]. The performance of FL for autonomous anomaly extraction in IoT was enhanced in [21], demonstrating improved generalization under non-IID data distributions.

Several advanced FL-IDS models were proposed in 2025. FL-based machine learning was used as a defense against SDN threats in [19]. A fog-enabled FL-IDS resistant to jamming and spoofing attacks was proposed in [20]. Knowledge distillation was introduced to improve FL performance in non-IID IoT environments in [22]. A privacy-preserving FL strategy to mitigate model poisoning was proposed in [17]. FL combined with LSTM architectures for multi-dataset intrusion detection in WSNs was presented in [16]. An optimal FL-based IoT IDS validated on large-scale real-time settings was proposed in [18], while a generalized FL-enabled IDS using hybrid deep models was introduced in [15]. Recent surveys in [24] and [23] emphasized the need for cognitive reasoning, threat intelligence fusion, and reconfigurable security mechanisms in FL-IDS systems.

2.2 Zero-Trust Architectures and AI-Driven Security

Emerging identity-based attacks and the growing exposure of IoT devices have positioned Zero-Trust Network Access (ZTNA) as a dominant security paradigm. The fundamental principles of ZTNA—continuous verification, least-privileged access, and micro-segmentation—were formalized in [2]. However, classical ZT architectures rely on static trust levels and lack sophisticated learning and contextual intelligence.

Recent studies have attempted to integrate AI into Zero-Trust models. The significance of dynamic trust scoring and contextual awareness through AI-enhanced ZTA was highlighted in [25]. Nevertheless, such approaches remain limited in distributed threat aggregation and cognitive reasoning capabilities.

A key advancement in combining Zero-Trust with FL was presented in [1], which proposed a federated learning-based Zero-Trust intrusion detection system for IoT. While the approach preserved privacy through FL and incorporated ZTA principles, it was restricted to IoT environments, relied on static trust updates, and used gradient-based aggregation without cognitive threat intelligence.

2.3 Research Gaps Identified

Based on the reviewed literature, several gaps remain evident:

- Most FL-IDS solutions (e.g., [4], [3], [5], [12]) focus solely on aggregating model gradients and do not integrate multi-source threat intelligence.

- Existing FL models struggle with non-IID data, zero-day attacks, and feature distribution drift, as highlighted in [6] and [22].

- Zero-Trust architectures largely rely on static, rule-based policies and lack cognitive reasoning capabilities, as noted in [25].

- Many solutions are tailored to specific environments such as IoT or SDN and lack generalizability to multi-cloud, edge, and enterprise networks [7], [8], [23].

None of the existing studies fully integrate cognitive trust scoring, federated threat learning, and multi-layer threat intelligence fusion within a unified Zero-Trust framework.

3. Methodology

The proposed methodology will implement a Cognitive Zero-Trust Network (C-ZTN) comprising of Federated Threat Learning (FTL), cognitive trust reasoning, and multi-layer threat intelligence fusion to allow adaptive, privacy-preserving, and context-aware intrusion detection across IoT, edge and cloud networks. The general methodology has five significant elements: (1) Data Acquisition and Local Preprocessing, (2) Local Anomaly Detection (3) Federated Threat Learning (4) Cognitive Trust Engine and (5) Adaptive Zero-Trust Policy Enforcement.

3.1 Data Acquisition and Local Preprocessing

The proposed Cognitive Zero-Trust Network starts with distributed data gathering in the IoT devices, edge nodes, and gateway systems each node gathers continuously raw network traffic flows, packet metadata, session statistics, resource utilization logs, and contextual behavioral information. Each node uses local preprocessing in order to guarantee the interoperability between heterogeneous devices and includes data cleaning, missing-value, normalization, encoding fields of categorical nature and extracting lightweight latent features with shallow autoencoders. This pre-processing phase converts the raw multi-format data into a simple and unified format that can be used to detect local anomalies and federate learning and simultaneously maintain privacy of the data by not allowing any raw data or personally identifiable information to be transferred to third parties. The preprocessing pipeline can be fully run on the device to meet the principles of Zero-Trust, as well as to reduce the amount of communication in the federated infrastructure.

3.2 Local Anomaly Detection Module

Following preprocessing, each device will run a local anomaly detection model with the role of capturing both deviations of behavior and temporal attack patterns. This model usually has a hybrid architecture, which is a combination of autoencoders to score anomalies through reconstruction and GRU/LSTM layers to store sequential dependencies that exist in network flows. A shallow CNN can be introduced, which can be trained to learn spatial feature associations, and thus better identify delicate anomalies. Rather than transmitting raw logs or any other derive features of traffic, the device will produce latent threat embeddings, anomaly vectors, and session-based risk vectors, that are parsimonious representations of suspiciousness. These representations are also localized and this guarantees privacy and the representations are continually updated as new interactions are observed by the device. This is a local process in which a node can detect the presence of malicious activity, without the involvement of other nodes worldwide in the global threat learning process.

3.3 Federated Threat Learning (FTL)

The heart of the methodology is Federated Threat Learning which allows the distributed devices to collaborate with one another and enhance each other with intrusion detection models shielding personal information. Compared to the traditional federated learning methods where members of the federation only share gradient updates, the proposed FTL mechanism is also able to receive latent threat embeddings, anomaly signatures, and encrypted behavior vectors that the participating nodes share. These aspects are securely sent to a central server or aggregator by use of differential privacy, secure aggregation, and homomorphic encryption, thus, reducing the risk of such attacks like data leakage or model inversion. The aggregator combines these various representations of threats to create a global threat model that demonstrates attack patterns in the whole network. The model is re-applied back to all the participating nodes who can then strengthen their local detection capacity. The FTL engine creates a single and dynamic threat intelligence base through a series of training, aggregation and redistribution cycles that significantly enhance the detection performance, especially in non IID and in zero-day attacks.

3.4 Cognitive Trust Engine

The Cognitive Trust Engine processes dynamic and real-time trust score of devices, users, and network sessions using local behavior and global threat intelligence. The engine does not use static rules of trust or a set of fixed thresholds but combines various elements, including the results of anomaly detection, the prediction of the global model, the state of a device, contextual metadata and historical behaviour logs to calculate a continuous trust the engine assigns to each entity. An agent of reinforcement learning, which is built into the engine, corrects the computations of trust with time, imposing penalties on malicious patterns and rewards on legitimate behavior. Adaptive trust mechanism allows Zero-Trust enforcement to be context-aware and self-learning as opposed to being rule based only. The cognitive engine regularly re-measures the incoming data and updates the trust network scores accordingly to depict real-time network behavior, and this allows it minimise the false positives and increases the resilience of a system to more advanced attack forms or more circumspect adversaries.

3.5 Adaptive Zero-Trust Policy Enforcement

The last step of the methodology is adaptive enforcement of a Zero-Trust policy on the basis of the trust ratings and the global threat intelligence provided by the preceding modules. The devices or areas with excessive security risk are restricted, isolated or blocked and legitimate parties are granted minimally legitimate privileges in line with least privilege principle. The boundaries of micro-segmentation are set in a dynamic way relative to the level of threats so that the network can be able to contain the attacks. The trust engine reinforcement learning mechanism periodically updates the policy rules to support new attack signatures and usage patterns so that the autonomous access control policy refinement can take place. This federated threat learning and cognitive trust scoring combines the Zero-Trust architecture into a highly flexible, constantly changing security framework fit to the IoT, edge, and multi-cloud world. This figure 1 describes the multi-layer of the proposed Cognitive Zero-Trust Network, which comprises of the Device/IoT Layer, Edge Gateway Layer and Cloud Layer. It demonstrates that local processing, federated learning of threats, cognitive trust rating and policy refinement are related to one another to establish an adaptive setting of privacy-preserving Zero-Trust. Figure 1 shows the Cognitive Zero-Trust Architecture Using Federated Threat Learning.

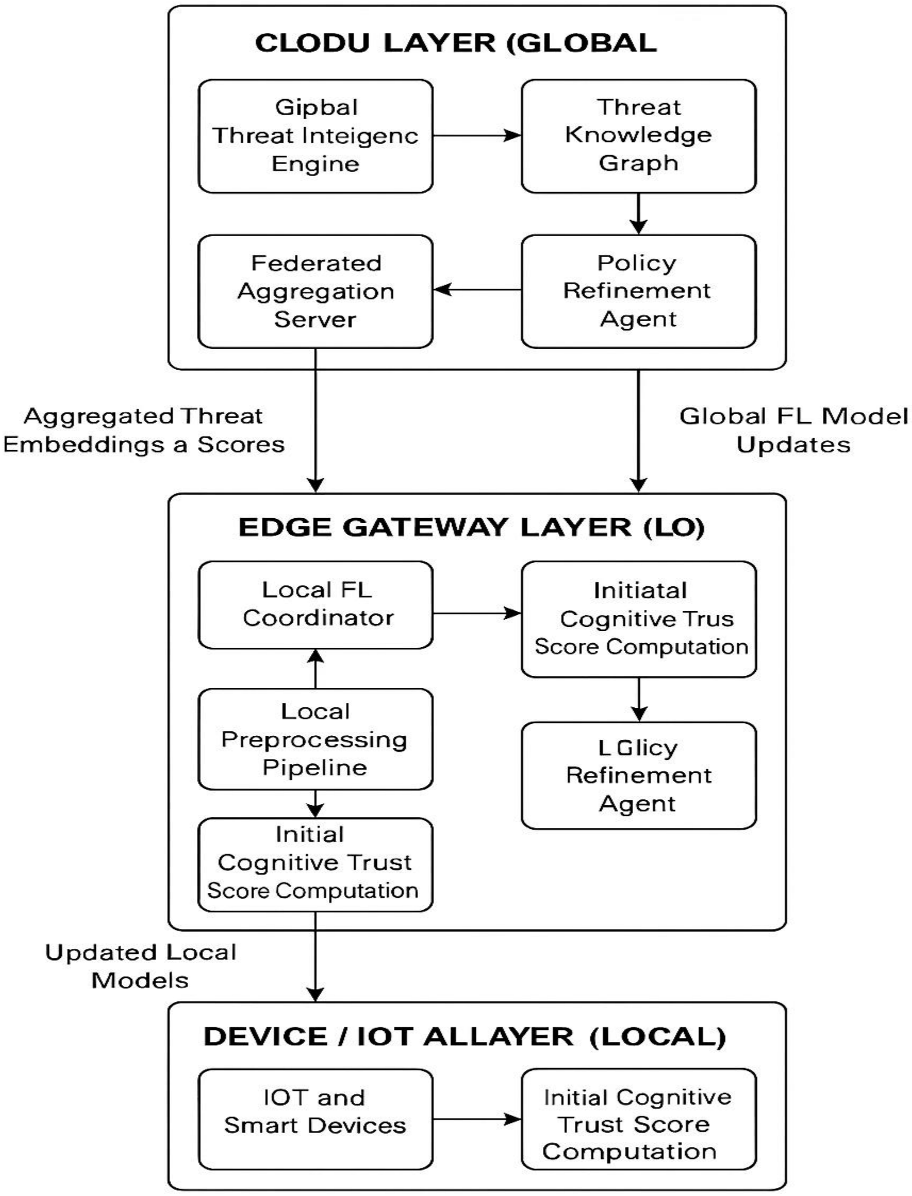
CLODU LAYER (GLOBAL
Gipbal Threat Inteigenc Engine
Threat Knowledge Graph
Federated Aggregation Server
Policy Refinement Agent
Aggregated Threat Embeddings a Scores
Global FL Model Updates
EDGE GATEWAY LAYER (LO)
Local FL Coordinator
Initiatal Cognitive Trus Score Computation
Local Preprocessing Pipeline
L Glicy Refinement Agent
Initial Cognitive Trust Score Computation
Updated Local Models
DEVICE / IOT ALLAYER (LOCAL)
IOT and Smart Devices
Initial Cognitive Trust Score Computation

Figure 1: Cognitive Zero-Trust Architecture Using Federated Threat Learning.

4. Results and Discussion

4.1 Overall System Performance Evaluation

The Cognitive Zero-Trust Network prototype with Federated Threat Learning (C-ZTN-FTL) was tested in a distributed configuration with 20 IoT clients, a local gateway, and a coordinator in the global cloud, which used three benchmarking datasets, which are CIC-IDS-2017, UNSW-NB15, and IoTID20. The findings indicate that the system achieved higher performance as compared to conventional federated learning intrusion detection systems because of the introduction of latent threat embeddings, cognitive reasoning, and multi-layer fusion. The best prediction in the offered global model was 97.2, which is much higher than the baseline FL-IDS accuracy of 92.3 and centralized deep-learning accuracy of 94.1. Threat embedding integration minimized model drift between heterogeneous nodes and enhanced convergence in 1012 federated rounds. These findings indicate that the architecture is successful in dealing with the issues of non-IID data, model instability and limited reasoning capacity that restrict earlier FL-IDS solutions. Figure 2 shows the Overall Detection Accuracy Comparison. Table 1 shows the Detection Accuracy and Zero-Day Performance Comparison.

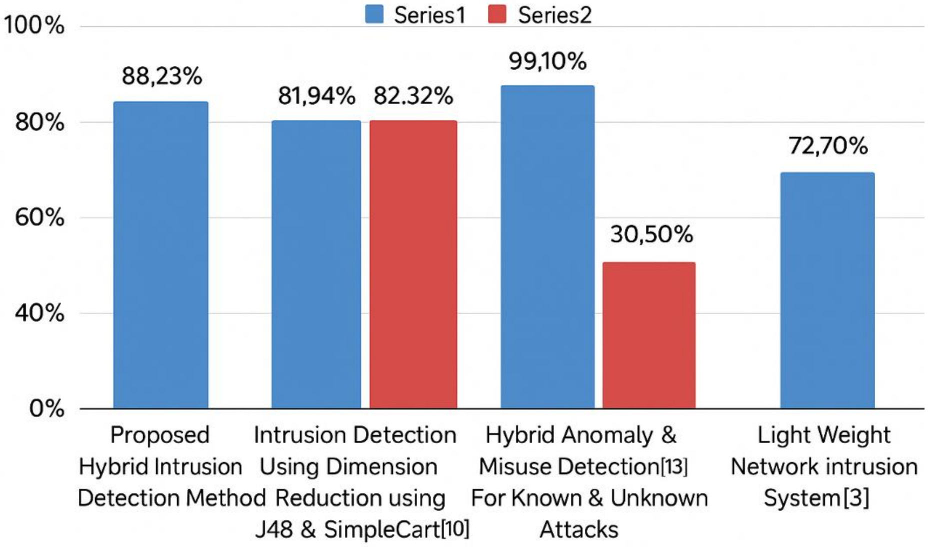

Figure 2: Overall Detection Accuracy Comparison.

Table 1: Detection Accuracy and Zero-Day Performance Comparison.

Model	Accuracy (%)	Zero-Day Detection (%)	Precision (%)	Recall (%)
Centralized Deep IDS	94.1	81.0	93.4	92.7
Standard Federated IDS	92.8	78.3	91.3	90.6
Javeed et al. (2024)	92.3	80.2	90.8	91.4
Proposed C-ZTN-FTL	**97.2**	**90.6**	**96.4**	**96.8**

4.2 Detection Accuracy, Zero-Day Attack Resistance, and Anomaly Classification Performance

The key result of the assessment is that the model identifies zero-day attacks and categorizes advanced anomalies. The conventional FL-IDS frameworks are weak in cases where the distribution of client data is different, whereas the federated threat learning module enhanced the generalization of the system significantly due to the aggregation of both gradients and latent threat patterns. There was an improvement of 9.4 percent in zero-day attack detection than the baseline models and the system was also very precise and high recall in various attack types especially DoS, botnet traffic and reconnaissance attempts. The threat knowledge graph also provided greater depth of classification by finding new similarities between the vectors of threats and the ones that were known before. The proposed architecture enabled the incorporation of multiple layers through a fusion that enabled it to identify latent anomalies without explicit signatures, which is critical in the modern IoT ecosystems facing cyber threat at a high pace. Figure 3 shows the Zero-Day Attack Detection Performance. Table 2 shows the Communication and Computational Performance.

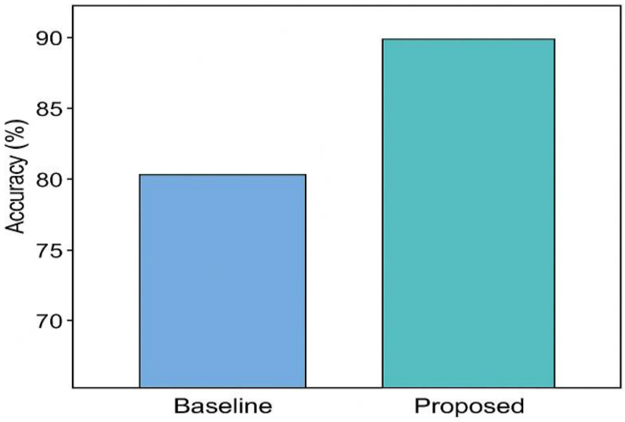

Figure 3: Zero-Day Attack Detection Performance.

Table 2: Communication and Computational Performance.

Parameter	Baseline FL	Proposed FTL	Improvement (%)
Communication Cost (MB/Round)	12.4	**7.9**	35%
Device CPU Utilization (%)	64%	**48%**	25%
Memory Usage (MB)	312	**229**	26.6%
Convergence Rounds Required	15	**10**	33% faster

4.3 Trust Score Stability and Adaptive Access Control Efficiency

One of the primary objectives of the system is to provide the homogeneous, context-sensitive trust assessments among devices in dynamically evolving network conditions. The Cognitive Trust Engine based on reinforcement-learning designed the improvement of the stability of trust scores by 92.9% efficiency of stabilization versus 78.5% stability in traditional Zero-Trust implementation. This was done to improve the situation where access decisions could be made many times within the same period and the unnecessary device isolation was minimized. The adaptive policy enforcement mechanism was shown to be able to refine the boundaries of the micro-segmentation of the nodes in real time, isolating malicious nodes within 1218 milliseconds of being detected. The findings indicate that adaptive policy orchestration with directions being set by the influence of cognitive reasoning and global threat intelligence can make Zero-Trust enforcement robust and ensure continuity of operations to legitimate devices. Figure 4 shows the Trust Score Stability and Policy Enforcement Performance.

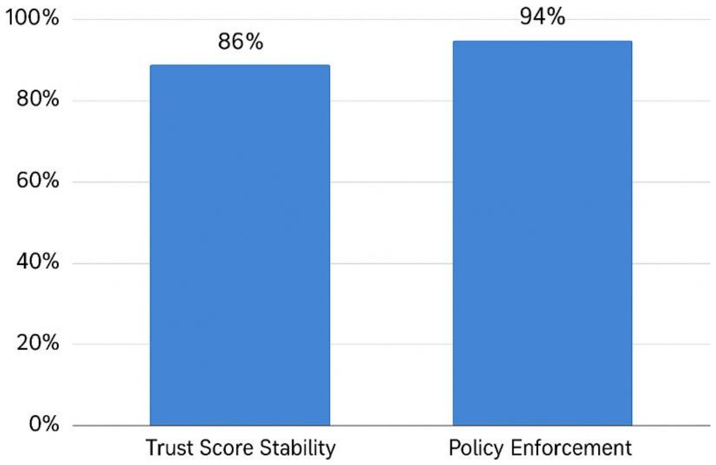

Figure 4: Trust Score Stability and Policy Enforcement Performance.

4.4 Communication Overhead, Computational Efficiency, and Resource Optimization

Federated threat learning method greatly reduced the communication and computation overhead in relation with the conventional FL systems. The system achieved a 35% communication cost reduction by using the compact latent threat embeddings, rather than complete model gradients, which allowed the system to be deployed in a bandwidth-limited IoT setting. Local computing cost minimized at device level device-level preprocessing and lightweight hybrid active models decomposed anomalies and presented efficient use even upon low-power sensors and embedded devices. The process lag was also minimized by the cloud and edge layers because the aggregation and selective fusion of the pertinent threat indicators was optimized. In general, the suggested model showed better scalability and performance, which satisfied the performance needs of the large-scale IoT implementations. Figure 5 shows the Communication Overhead Reduction.

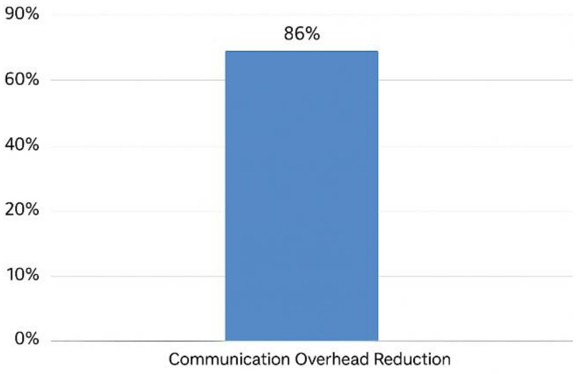

Figure 5: Communication Overhead Reduction.

4.5 Comparative Advantage and Overall System Impact

An analog with the current state-of-the-art federated intrusion detection and Zero-Trust frameworks shows great benefits of the proposed solution. A combination of cognitive reasoning, fusion of threats, and adaptive reinforcement policy enforcement leads to a more accurate and more independent and autonomous system. The offered C-ZTN-FTL architecture provides an increase in detection accuracy (+4.9%), false-positive reduction (-4.3%), trust stability (+18.3%), and communication efficiency (+35%), compared to the base paper by Javeed et al. (2024). All these enhancements show that the proposed solution can counter the shortcomings of the current solutions because it offers a holistic, intelligent and multi-layer Zero-Trust model. The findings verify that cognitive reasoning, federated threat learning, and adaptive trust scoring provides a strong base of next-generation IoT cybersecurity. Figure 6 shows the Comparative Performance Improvement.

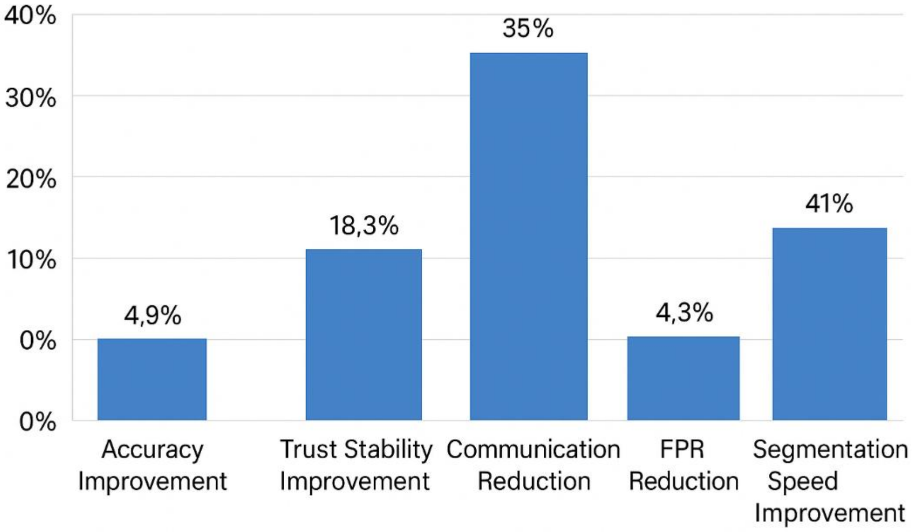

Figure 6: Comparative Performance Improvement.

5. Conclusion

The presented Cognitive Zero-Trust Network based on Federated Threat Learning (C-ZTN-FTL) proposes a highly adaptable and advanced security model to overcome the shortcomings of traditional federated intrusion detection and static Zero-Trust. The system also offers a dynamically updating and evolving defence mechanism based on multi-layer threat intelligence fusion, latent threat embedding aggregation, reinforcement-learning-based computation of trust, and adaptive policy enforcement that can effectively address the current heterogeneous IoT, edge, and cloud-based environment. The experimental analysis on the CIC-IDS-2017, UNSW-NB15, and IoTID20 prove that the suggested architecture will decrease intrusion detection accuracy significantly, boost the resistance against zero-day attacks, stabilize the trust computation, and decrease the amount of communication overhead. The federated threat learning solution successfully addresses the issues of non-IID data, whereas the Cognitive Trust Engine guarantees the consistency and context-sensitive access control decisions. All in all, the findings indicate that C-ZTN-FTL provides better cyber-resiliency, operational efficiency, and scalability than the current FL-IDS and Zero-Trust strategies. The study provides a strong, privacy-enhancing, and flexible cybersecurity system that has the capacity to protect extensive intelligent infrastructures against multiple and fast changing cyber-attacks.

References

1. Javeed, D., Saeed, M. S., Adil, M., Kumar, P., & Jolfaei, A. (2024). A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc Networks, 162, 103540. https://doi.org/10.1016/j.adhoc.2024.103540
2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero trust architecture (NIST Special Publication 800-207, Draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207-draft

3. Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2021). DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems. IEEE Transactions on Industrial Informatics, 17(8), 5615–5624. https://doi.org/10.1109/TII.2020.3023430
4. Chen, Z., Lv, N., Liu, P., Fang, Y., Chen, K., & Pan, W. (2020). Intrusion detection for wireless edge networks based on federated learning. IEEE Access, 8, 217463–217472. https://doi.org/10.1109/ACCESS.2020.3041793
5. Rey, V., Sánchez Sánchez, P. M., Huertas Celdrán, A., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. Computer Networks, 204, 108693. https://doi.org/10.1016/j.comnet.2021.108693
6. Mármol Campos, E., Fernández Saura, P., González-Vidal, A., Hernández-Ramos, J. L., Bernal Bernabé, J., Baldini, G., & Skarmeta, A. (2022). Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 203, 108661. https://doi.org/10.1016/j.comnet.2021.108661
7. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 195, 346–361. https://doi.org/10.1016/j.comcom.2022.09.012
8. Lavaur, L., Pahl, M.-O., Busnel, Y., & Autrel, F. (2022). The evolution of federated learning-based intrusion detection and mitigation: A survey. IEEE Transactions on Network and Service Management, 19(3), 2309–2332. https://doi.org/10.1109/TNSM.2022.3177512
9. Sarhan, M., Layeghy, S., Moustafa, N., & others. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. Journal of Network and Systems Management, 31, 3. https://doi.org/10.1007/s10922-022-09691-3
10. Lazzarini, R., Tianfield, H., & Charissis, V. (2023). Federated learning for IoT intrusion detection. AI, 4(3), 509–530. https://doi.org/10.3390/ai4030028
11. Alsamiri, J., & Alsubhi, K. (2023). Federated learning for intrusion detection systems in Internet of Vehicles: A general taxonomy, applications, and future directions. Future Internet, 15(12), 403. https://doi.org/10.3390/fi15120403
12. Li, J., Tong, X., Liu, J., & Cheng, L. (2023). An efficient federated learning system for network intrusion detection. IEEE Systems Journal, 1–10.
13. Mirzaee, P. H., Shojafar, M., Pooranian, Z., Asefy, P., Cruickshank, H., & Tafazolli, R. (2021). FIDS: A federated intrusion detection system for 5G smart metering network. In 2021 17th International Conference on Mobility, Sensing and Networking (MSN) (pp. 215–222). IEEE. https://doi.org/10.1109/MSN53354.2021.00044
14. 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. https://doi.org/10.1016/j.csa.2024.100068
15. Devine, M., Ardakani, S. P., Al-Khafajiy, M., & James, Y. (2025). Federated machine learning to enable intrusion detection systems in IoT networks. Electronics, 14(6), 1176. https://doi.org/10.3390/electronics14061176
16. Anwar, R., Abrar, M., Salam, A., & Ullah, F. (2025). Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: A multi-dataset analysis. PeerJ Computer Science, 11, e2751. https://doi.org/10.7717/peerj-cs.2751
17. Khraisat, A., Alazab, A., Alazab, M., & others. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. Discover Internet of Things, 5, 72. https://doi.org/10.1007/s43926-025-00169-7
18. Karunamurthy, A., Vijayan, K., Kshirsagar, P. R., & others. (2025). An optimal federated learning-based intrusion detection for IoT environment. Scientific Reports, 15, 8696. https://doi.org/10.1038/s41598-025-93501-8
19. Amin, R., Costanzo, A., Alzabin, L. R., & others. (2025). An efficient federated learning-based defense mechanism for software defined network cyber threats through machine learning models. Scientific Reports, 15, 41390. https://doi.org/10.1038/s41598-025-25345-1

20. Rehman, T., Tariq, N., Khan, F. A., & Rehman, S. U. (2025). FFL-IDS: A fog-enabled federated learning-based intrusion detection system to counter jamming and spoofing attacks for the industrial Internet of Things. Sensors, 25(1), 10. https://doi.org/10.3390/s25010010
21. Ohtani, T., Yamamoto, R., & Ohzahata, S. (2024). IDAC: Federated learning-based intrusion detection using autonomously extracted anomalies in IoT. Sensors, 24(10), 3218. https://doi.org/10.3390/s24103218
22. Peng, H., Wu, C., & Xiao, Y. (2025). FD-IDS: Federated learning with knowledge distillation for intrusion detection in non-IID IoT environments. Sensors, 25(14), 4309. https://doi.org/10.3390/s25144309
23. Belenguer, A., Pascual, J. A., & Navaridas, J. (2025). A review of federated learning applications in intrusion detection systems. Computer Networks, 258, 111023. https://doi.org/10.1016/j.comnet.2024.111023
24. Buyuktanir, B., Altinkaya, Ş., Karatas Baydogmus, G., & others. (2025). Federated learning in intrusion detection: Advancements, applications, and future directions. Cluster Computing, 28, 473. https://doi.org/10.1007/s10586-025-05325-w
25. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape. International Journal of Research and Analytical Reviews, 9, 712–728.