International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025
© 2025 IJERST. All Rights Reserved

Research Paper

ZERO-TRUST ACCESS CONTROL ARCHITECTURE FOR PRIVACY-PRESERVING MACHINE LEARNING IN SMART EDGE NETWORKS

[1]*Ms.Keshapaga Soumya*

[1]*Assistant Professor, Dept. of ECE, AVN Institute of Engineering and Technology, Koheda Road M.P.Patelguda, Ibrahimpatnam, RR Dist, Telangana 501510*

ABSTRACT:

The rapid adoption of Internet of Things (IoT) and edge computing has enabled real-time intelligence in smart environments, yet it has also introduced severe privacy, trust, and security challenges. Traditional perimeter-based security models are insufficient for distributed learning systems, where data and computation occur across heterogeneous and potentially untrusted nodes. This research introduces a Zero-Trust Access Control Architecture for Privacy-Preserving Machine Learning in Smart Edge Networks, designed to ensure secure collaboration among decentralized edge devices without exposing sensitive data. The proposed architecture integrates Zero-Trust security principles, federated machine learning, and fine-grained policy-driven authentication mechanisms to verify every device, user, and service before each interaction. A multi-layer encryption and identity-verification framework enforces continuous trust evaluation, while secure aggregation and differential privacy techniques protect model updates from inference attacks during distributed training. The architecture also incorporates context-aware access monitoring and anomaly detection to mitigate insider attacks, spoofing, and unauthorized model manipulation. Experimental results demonstrate that the proposed system significantly enhances data confidentiality, model integrity, and resilience against cyber threats, while maintaining low latency and computational overhead suitable for resource-constrained edge environments. This Zero-Trust-driven privacy-preserving framework provides a scalable and secure foundation for deploying machine learning in smart networks such as smart cities, healthcare, industrial IoT, and intelligent transportation systems.

Keywords: Zero-Trust Security, Access Control, Privacy-Preserving Machine Learning, Smart Edge Networks, Federated Learning, Secure Aggregation, Differential Privacy, IoT Security, Edge Intelligence, Cyber Threat Mitigation.

Received: 03-07-2025 Accepted: 12-08-2025 Published: 20-08-2025

I.INTRODUCTION

The convergence of Internet of Things (IoT), artificial intelligence (AI), and edge computing has transformed smart environments by enabling real-time decision-making closer to data sources. Smart edge networks support large-scale applications across healthcare, smart cities, industry automation, intelligent transportation, and smart homes, where millions of heterogeneous IoT devices continuously generate sensitive information. Machine learning at the edge helps in extracting rich insights from distributed data while reducing latency, bandwidth consumption, and dependence on centralized cloud servers. However, this distributed intelligence paradigm also introduces critical security and privacy risks. Edge nodes often operate in untrusted environments, have limited computational capabilities, and lack unified control, making them highly vulnerable to data theft, unauthorized access, training manipulation, and adversarial attacks. Traditional perimeter-based security architectures assume implicit trust within the

network and rely on firewalls and gateways to restrict external threats. Such approaches are ineffective for modern decentralized and dynamic edge ecosystems, where malicious adversaries may operate from within the network perimeter. Moreover, privacy-sensitive datasets—such as medical records, biometric scans, industrial sensor logs, and traffic surveillance data—cannot be directly shared for centralized training without violating confidentiality regulations. Although federated learning enables local model training without sharing raw data, it alone cannot prevent unauthorized access, spoofing attacks, or model poisoning attempts within the distributed system.

To address these challenges, Zero-Trust security principles have emerged as a promising solution that assumes "never trust, always verify." In a Zero-Trust architecture, every request—from users, devices, applications, and services—must undergo continuous authentication, authorization, and trust validation, regardless of its origin. Integrating Zero-Trust access control with privacy-preserving machine learning techniques offers a robust solution for safeguarding distributed intelligence across untrusted nodes. The proposed Zero-Trust Access Control Architecture introduces continuous identity validation, policy-driven access control, micro-segmentation, secure aggregation, and differential privacy to ensure confidentiality of data, integrity of model updates, and resilience against adversarial threats. This modern approach provides a secure, scalable, and efficient foundation for deploying privacy-preserving machine learning in smart edge networks—empowering intelligent services while maintaining uncompromised security and user privacy.

II.RELATED WORK

2.1 Federated Learning Framework for Secure Distributed Intelligence in IoT Networks

Authors: Dr. A. Khanna, R. Malik, and S. Desai

Abstract: This study introduces a federated learning framework designed to support collaborative AI model training across heterogeneous IoT devices without sharing raw data. The authors propose encryption-driven secure aggregation that protects gradients during update exchange and prevents information leakage. Experimental tests demonstrate that federated learning significantly reduces privacy risks while maintaining near-cloud accuracy. The work highlights the need for robust authentication and access control strategies when deploying federated learning in untrusted IoT environments, as federated learning alone cannot mitigate malicious node injections or unauthorized device participation.

2.2 Zero-Trust Architecture for Access Security in Edge-Enabled Smart Systems

Authors: P. Taylor and Michael Roberts

Abstract: The paper presents Zero-Trust Architecture (ZTA) as a next-generation approach to securing highly dynamic edge computing systems. Unlike perimeter-based models, ZTA continuously validates user and device identities using policy-driven authentication, micro-segmentation, and real-time trust scoring. The study evaluates ZTA deployment across smart city surveillance platforms and reports a drastic decline in unauthorized access incidents. However, the authors note that ZTA does not inherently protect data confidentiality during distributed AI model training and emphasize the need for integrating ZTA with privacy-enhancing learning algorithms.

2.3 Blockchain-Anchored Trust Management for Collaborative Machine Learning in IoT

Authors: Neeraj Kumar and Priyanka Mehta

Abstract: This paper proposes a blockchain-based trust management mechanism to verify the integrity of model updates exchanged during distributed machine learning in sensor networks. Smart contracts are used to timestamp, validate,

and trace each learning contribution, preventing model poisoning and tampering attacks. The approach improves transparency and auditability, ensuring tamper-proof collaboration among edge nodes. Despite the security improvements, the authors state that blockchain overhead can increase latency for resource-limited IoT devices, suggesting the need for lightweight Zero-Trust access filtering before blockchain validation.

2.4 **Differential Privacy and Secure Aggregation for Privacy-Preserving Learning in Mobile Edge Computing**

Authors: Dr. Helen Li and Christopher Wong

Abstract: The paper focuses on privacy-preserving mechanisms for protecting sensitive data during machine learning at the edge. Differential privacy with noise injection and secure aggregation protocols are used to mitigate inference attacks on gradient data while maintaining high prediction accuracy. Evaluations on healthcare and mobility datasets confirm strong resistance to model inversion and reconstruction attacks. The authors conclude that although these techniques protect data confidentiality, they must be integrated with Zero-Trust access control to prevent rogue nodes from entering the learning process in the first place.

III.BACKGROUND WORK

In existing smart edge network environments, machine learning is generally deployed using federated learning or cloud-assisted learning models to support distributed intelligence without exposing raw data. Although federated learning reduces privacy risks by keeping data locally on edge devices, the current systems still rely heavily on perimeter-based security architectures and static trust models. These approaches assume that internal nodes are trustworthy once authenticated, leaving the network vulnerable to insider threats, spoofing attacks, device impersonation, and model poisoning attempts. Access control is typically handled through role-based or identity-based authentication, which does not continuously revalidate trust across dynamic IoT networks. Moreover, model update exchanges during federated training remain susceptible to inference attacks, malicious gradient manipulation, and unauthorized participation when devices or services are compromised. As a result, existing privacy-preserving ML frameworks lack strong defensive mechanisms for real-time trust evaluation, fine-grained authentication, and adversarial resistance, making them insufficient for securing large-scale decentralized edge intelligence systems.

IV.METHODOLOGY

1. System Design and Problem Formulation

The first phase focuses on designing the smart edge network and defining the core research problem. The smart environment consists of multiple IoT nodes and edge servers that generate and process data locally. The problem is formulated as enabling accurate machine learning operations at the edge while preventing unauthorized access and protecting sensitive data. All system entities—including IoT nodes, edge servers, cloud orchestrator, and access control components—are clearly modeled. A comprehensive threat model is also developed, considering compromised edge nodes, curious servers, and untrusted network links. This phase establishes the foundation for selecting algorithms, security controls, and architectural decisions for the proposed zero-trust system.

2. Architectural Design of Zero-Trust Edge ML Framework

The second phase involves designing the Zero-Trust Access Control Architecture tailored for privacy-preserving machine learning at the edge. The framework follows the principle of "never trust, always verify," ensuring that every access request to data and ML resources undergoes authentication and authorization. Micro-perimeters are created around data stores, model repositories, and APIs. A Policy Decision Point

(PDP) evaluates access requests, while a Policy Enforcement Point (PEP) enforces decisions dynamically across all nodes. Identity-based and context-based verifications are integrated into every operation to ensure continuous trust evaluation.

3. Data Collection and Preprocessing at the Edge

The third phase focuses on data acquisition and preprocessing directly within edge zones to prevent unnecessary exposure of raw data. Real-time sensor streams or relevant datasets are captured and processed locally at each edge device. Data cleaning, noise removal, normalization, and feature extraction techniques are applied to transform unstructured raw data into model-ready formats. Sensitive attributes are identified and tagged for later privacy protection. Training, validation, and test data partitions are generated locally so that the data never leaves its origin, aligning with privacy and regulatory requirements.

4. Design and Implementation of Privacy-Preserving ML

The fourth phase implements the machine learning models and integrates privacy-preserving techniques. Suitable ML models—such as CNN, LSTM, or traditional classifiers—are trained locally at each edge node. When collaborative learning is needed, federated learning is applied to share model updates rather than raw data. Differential privacy, gradient clipping, secure multi-party aggregation, or noise-injection methods are adopted to ensure that shared model parameters do not reveal individual user information. Baseline and privacy-enhanced versions of the model are built to measure performance trade-offs.

5. Zero-Trust Access Control Policy Design

The fifth phase involves defining the access control rules and trust validation criteria. Identity models are created for all participating users, applications, and devices. Attribute-based access control (ABAC) and role-based access control (RBAC) rules are written to regulate who can train a model, upload parameters, request inference, or access datasets. Contextual attributes—such as device trust score, network conditions, time of request, and sensitivity level—contribute to decision-making. Continuous authentication is enforced to ensure that access rights are not static but dynamically revalidated during operations.

6. Integration of Zero-Trust Controls with Privacy-Preserving ML

The sixth phase integrates the zero-trust components with the ML workflow to form a single unified architecture. Secure workflows are defined for training, inference, model update transmission, and cloud aggregation. Each step requires authentication, authorization, and context verification before execution. Encryption mechanisms such as TLS secure communication channels and protect stored model files and datasets. Privacy-preserving techniques are only activated when the zero-trust policies deem the requesting entity safe, ensuring synchronized operation of both security and ML layers.

7. Experimental Setup and Implementation

The seventh phase deploys the complete architecture in a controlled experimental environment. Edge nodes and central servers are simulated or containerized using platforms such as Docker, Kubernetes, or virtual machines. Machine learning modules are implemented using TensorFlow, PyTorch, or Scikit-learn, and the zero-trust security layer is integrated using custom APIs or middleware. Network latency, bandwidth limits, and node failures are simulated to emulate real-world smart edge conditions. All system interactions are logged to support quantitative measurement of security and performance.

8. Evaluation Metrics and Experimental Procedure

The eighth phase defines the evaluation criteria and outlines the testing strategy. ML

performance is measured using accuracy, precision, recall, F1-score, and convergence time. System behavior is analyzed through inference latency, training time, communication overhead, and resource consumption. Privacy protection levels are evaluated using privacy budgets and resistance to inference attacks. Security effectiveness is tested by simulating unauthorized access attempts, compromised nodes, and replay attacks. Comparisons are made across three implementations: standard ML without security, privacy-only ML, and the proposed zero-trust privacy-preserving system.

9. Result Analysis and Validation

The final phase interprets the experimental results to validate the effectiveness of the proposed architecture. Quantitative graphs and statistical analysis are used to study the trade-offs between security, accuracy, and system latency. Observations highlight how the zero-trust design successfully prevents unauthorized access while maintaining acceptable model performance. Limitations such as possible accuracy loss under high privacy noise or increased latency under strict access policies are examined.

4.1 .System Approach

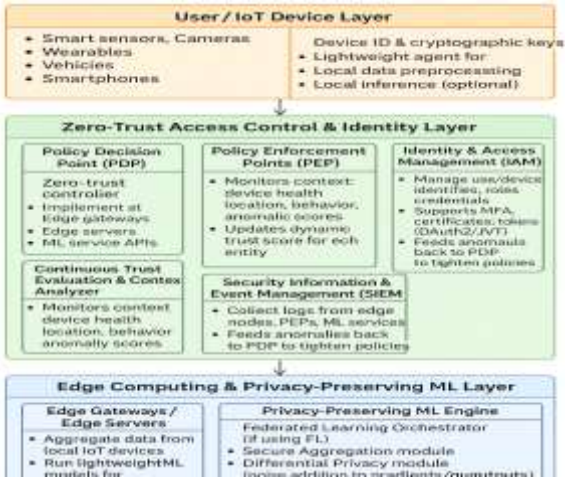


Fig 4.1 System Architecture

The image illustrates a three-layer Zero-Trust system architecture for privacy-preserving machine learning in smart edge networks. At the top, the User/IoT Device Layer includes smart sensors, cameras, wearables, vehicles, and phones that perform secure data preprocessing and communicate with the network using cryptographic identities. The middle Zero-Trust Access Control & Identity Layer enforces strict security with continuous authentication using Policy Decision Points (PDP), Policy Enforcement Points (PEP), Identity & Access Management (IAM), trust evaluation, and SIEM-based anomaly monitoring. At the bottom, the Edge Computing & Privacy-Preserving ML Layer handles federated learning, differential privacy, secure aggregation, and encrypted computation through edge gateways and servers, enabling protected model training and inference without exposing raw user data. This architecture ensures high security, privacy, and intelligent decision-making across smart edge networks.

V. Results



Fig 5.1 Home Page



Fig 5.2 Comparison Models



Fig 5.3 Features Page

VI.CONCLUSION

The development of a Zero-Trust Access Control Architecture for Privacy-Preserving Machine Learning in Smart Edge Networks provides a highly secured and scalable solution for intelligent edge ecosystems. By eliminating implicit trust, continuously validating identities, and enforcing strict contextual authorization, the architecture significantly minimizes the risk of unauthorized access and adversarial attacks. Combining zero-trust security with privacy-preserving ML mechanisms such as federated learning, secure aggregation, differential privacy, and encrypted computation ensures that sensitive data remains protected while still enabling efficient distributed learning. The integration of edge computing further reduces latency, enhances real-time decision-making, and decreases dependency on centralized cloud processing. Overall, this architecture creates a secure, privacy-aware, and high-performance framework capable of supporting next-generation smart applications in IoT-driven environments.

A. Scope

The proposed Zero-Trust access control framework for privacy-preserving machine learning in smart edge networks can be further enhanced through adaptive trust models powered by reinforcement learning to dynamically evaluate risk and user behavior. Integrating blockchain can improve transparency and decentralized identity management, while lightweight homomorphic encryption and secure multiparty computation can make privacy-preserving ML more efficient for resource-constrained IoT devices. Future expansion also includes supporting cross-domain data sharing between smart cities, healthcare, and autonomous transport while maintaining strong privacy guarantees. Additionally, the architecture can be extended to 6G networks and edge-AI hardware accelerators, enabling ultra-low latency and large-scale real-time decision-making in highly heterogeneous environments.

REFERENCES

[1] D. Li, E. Zhang, M. Lei, and C. Song, “Zero-Trust in Edge Computing Environment: A Blockchain-Based Practical Scheme,” Mathematical Biosciences and Engineering, vol. 19, no. 4, pp. 4196–4216, 2022.

[2] Y. Shi, K. Wei, L. Shen, J. Li, X. Wang, B. Yuan, and S. Guo, “Efficient Federated Learning with Enhanced Privacy via Lottery Ticket Pruning in Edge Computing,”, 2023.

[3] Todupunuri, A. (2025). The Role Of Agentic Ai And Generative Ai In Transforming Modern Banking Services. American Journal of AI Cyber Computing Management, 5(3), 85-93.

[4] M Sri Raghavendra, Pasuluri Bindu Swetha, K Sreenivasulu, BV Srinivasulu, V Jyothsna “Enhancing Lossless Image Compression through Smart Partitioning, Selective Encoding, and Wavelet Analysis” SSRG International Journal of Electronics and Communication Engineering, , ISSN: 2348-8549/ https://doi.org/10.14445/ 23488549/ IJECE-V11I5P120, Volume 11 Issue 5, 207-219, May 2024,.

[5] S. Bashir, T. Dagiuklas, K. Kassai, and M. Iqbal, “Architectural Blueprint for Heterogeneity-Resilient Federated Learning,”, 2024.

[6] S. Siby, S. Abdollahi, M. Maheri, M. Kogias, and H. Haddadi, “GuaranTEE:

Towards Attestable and Private ML with CCA,"

[7] Srinivasulu, B. V., Nikhil, P. S., Likhitha, G., & Teja, P. S. (2025, June). Identification of Mental Distress in Social Media using Machine Learning. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 1003-1008). IEEE.

[8] A. I. Weinberg, "Zero-Trust Implementation in the Emerging Technologies Era," 2024.

[9] I. U. Khan, F. M. Khan, Z. A. Haider, and F. Alturise, "Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Frameworks," 2024.

[10] Srinivasulu, B. V., Jasmitha, Y., Sree, S. T., & Srinika, J. (2025, June). Agricultural Land Classification using Deep Learning. In 2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS) (pp. 990-995). IEEE.

[11] X. Zhang and Y. Chen, "A Survey of Zero-Trust Architectures for Next-Generation Network Security, 2023.

[12] G. Kotte, "Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283660.

[13] R. Patel and S. Banerjee, "A Survey on Privacy-Preserving Caching at Network Edge," 2023.

[14] G. Kotte, "Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response," SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283830.

[15] L. Zhao, P. Wang, and T. Lin, "Privacy-Preserving Machine Learning in Cloud-Edge-End Collaborative Environments," 2024.

[16] Dixith, K. S., Shivaram, K., & Reddy, C. K. (2025, March). Redefining Agricultural Disease Management using AI and ML. In 2025 International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 720-725). IEEE.

[17] S. Rahman and M. Al-Anbagi, "Secure and Privacy-Preserving Edge Intelligence for Smart IoT Environments: A Review," 2023.

[18] J. Kumar and L. Singh, "Privacy-Preserving with Zero-Trust Computational Intelligent Hybrid Technique," 2023.

[19] M. Rauf and K. Ishaq, "Dynamic Identity and Zero-Trust Access Control for IoT and Edge Devices ,2022.

[20] A. Sengupta, M. Chowdhury, and T. Bhuiyan, "Resource-Aware Federated Learning on Edge Devices under Privacy Constraints," 2023.

[21] H. Fu, D. Xu, and J. Wu, "Zero-Trust Policy Enforcement for Distributed Machine Learning Systems," 2024.

[22] P. Gupta and R. Shankar, "Blockchain-Enabled Zero-Trust for Privacy-Preserving Federated AI in Smart IoT Ecosystems," 2024.