Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Leveraging Federated Learning and Edge Computing for Privacy-Preserving Real-Time Anomaly Detection in IoT Networks

Arpan Hendri Batuara[1], Sri Jenni Rejeki Situringkir[2], Rangga Ramadia[3], Richand Pamilano[4], Sinek Mehuli BR Perangin Angin[5], Devita Permata Sari BR Ginting[6]
Institut Teknologi dan Bisnis Indonesia, Indonesia

Article Info
Keywords:
IoT,
Networks,
Computing

ABSTRACT
The rapid proliferation of Internet of Things (IoT) networks has heightened the need for robust, privacy-preserving security mechanisms that ensure real-time anomaly detection. This article explores the integration of federated learning (FL) and edge computing as a promising approach to address challenges related to privacy, latency, and resource constraints in IoT environments. Employing a qualitative research methodology, this study analyzes existing literature and emerging frameworks to comprehensively assess the advantages, challenges, and future research directions of applying FL and edge computing for anomaly detection in IoT. Findings highlight that FL combined with lightweight anomaly detection algorithms deployed at the edge can significantly enhance privacy while ensuring timely intrusion detection, despite heterogeneity and limited device resources. The study suggests pathways for developing adaptive, scalable, and secure IoT networks leveraging these paradigms.

Corresponding Author:
Sinek Mehuli Br Perangin Angin
Institut Teknologi dan Bisnis Indonesia, Indonesia
sinekmehulibrperanginangin@itbi.ac.id

INTRODUCTION

The Internet of Things (IoT) represents one of the most transformative technological revolutions of the modern era, integrating billions of heterogeneous devices into pervasive networks that collect, transmit, and analyze vast amounts of data in real time. These devices, ranging from industrial sensors and smart home appliances to healthcare wearables and autonomous vehicles, generate multi-dimensional data streams that facilitate improved automation, intelligent decision-making, and new services across various domains. According to recent reports, the volume of data produced at the network edge — that is, the point where devices interact with the physical environment — is projected to reach multiple zettabytes annually, reflecting an explosion of decentralized information that presents unprecedented opportunities and challenges (Mughal et al., 2024).

Central to realizing the promise of IoT is the capability to detect anomalous behaviors or cybersecurity threats in real time, thereby safeguarding system integrity and ensuring operational reliability. Anomaly detection is critical for identifying events such as malicious intrusions, equipment malfunctions, or unexpected environmental changes. Traditional approaches to anomaly detection rely heavily on centralized data aggregation and analysis in the cloud or data centers. While these centralized frameworks benefit from robust

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

computational resources, they introduce significant drawbacks. The aggregation of sensitive raw data at a central server heightens privacy risks, increases latency, and demands substantial bandwidth. These inefficiencies hinder timely responses and expose IoT ecosystems to data breaches, raising stringent regulatory and ethical concerns, particularly when personal or proprietary data is involved (Mahesh Kolli, 2025).

Edge computing has emerged as a promising paradigm to alleviate the constraints of centralized architectures by relocating data processing and analytics from centralized cloud servers to localized edge nodes proximal to data sources. This shift toward decentralized processing significantly reduces communication overhead and latency, accelerating inference tasks essential for real-time anomaly detection in IoT deployments. Edge devices, empowered by embedded computational capabilities, can perform preliminary data filtering, feature extraction, and localized decision-making, which enhances scalability and resilience across distributed networks (Tiwari et al., 2023).

Nevertheless, edge computing alone does not fully resolve critical concerns related to privacy preservation and collaborative intelligence across diverse IoT nodes. The heterogeneity of IoT devices—with variations in data quality, computational power, and connectivity—poses additional complexities in designing efficient, adaptive anomaly detection systems. Moreover, direct sharing of raw data between edge nodes or with central aggregators remains fraught with security vulnerabilities, limiting cross-device cooperation crucial for building robust detection models (Odeh et al., 2025).

Federated Learning (FL) has recently gained traction as a transformative distributed machine learning framework that addresses the dual challenges of privacy and collaboration within IoT and edge computing ecosystems. Unlike traditional centralized learning where data is pooled at a central server for model training, federated learning facilitates decentralized model development by enabling devices to locally train shared machine learning models on their private data and communicate only model updates, such as gradients or weights, to a coordinating server. This approach effectively retains the raw data on edge devices, mitigating privacy risks and reducing communication bandwidth requirements (Alasbali et al., 2025).

The integration of federated learning with edge computing presents a synergistic paradigm that harnesses the computational power of edge devices while maintaining stringent privacy guarantees. In this decentralized setting, edge nodes collaboratively improve a global anomaly detection model by exchanging encrypted and aggregated model parameters, employing advanced cryptographic techniques such as secure multi-party computation and homomorphic encryption to further obfuscate sensitive information during transmission. This combination allows real-time, privacy-preserving anomaly detection to be executed close to the data sources, facilitating rapid responses to emergent threats without compromising data sovereignty or system efficiency.

Recent advancements in federated learning algorithms and architectures have addressed key challenges in deploying such systems in IoT networks. These challenges include handling non-independent and identically distributed (non-IID) data, contending with variable device reliability and availability, optimizing communication overhead, and achieving

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

convergence in heterogeneous and resource-constrained environments. Techniques such as asynchronous model aggregation, hierarchical federated learning across multiple edge layers, and adaptive node selection strategies have enhanced the robustness and scalability of federated learning systems in industrial and consumer IoT settings.

Moreover, the incorporation of sophisticated anomaly detection models—such as federated hybrid deep belief networks, temporal convolutional networks, and adversarial federated networks—has significantly improved detection accuracy while preserving privacy. These models can efficiently extract temporal and spatial patterns from time-series IoT data streams, which are crucial for distinguishing benign from anomalous events in dynamic real-world environments. In addition, advances in model compression and quantization enable these complex models to be deployed on IoT edge devices with limited computational resources, thereby bridging the gap between theoretical performance and practical applicability.

The qualitative synthesis of prior research and empirical findings confirms that federated learning and edge computing jointly constitute a powerful paradigm for privacy-preserving, scalable, and real-time anomaly detection tailored for the next-generation IoT networks. They reduce the reliance on centralized infrastructures, safeguard sensitive data, accommodate the diversity of IoT ecosystems, and enable timely detection and mitigation of cyber threats and operational anomalies.

METHODS

This study uses a qualitative research design centered on a systematic literature review and thematic analysis of contemporary academic publications, technical reports, and case studies addressing federated learning (FL) and edge computing (EC) frameworks for privacy-preserving real-time anomaly detection in Internet of Things (IoT) networks. Given the recent surge in research intersecting these domains, qualitative synthesis allows for an in-depth understanding of the methods, challenges, and innovations that characterize the state-of-the-art.

Qualitative analysis is particularly suitable as it supports interpretive examination of complex, interdisciplinary technological concepts, including privacy preservation mechanisms, distributed machine learning architectures, cryptographic techniques, and edge-based resource constraints. It enables identifying emerging patterns and contextualizing research gaps and practical challenges in deploying FL-edge systems tailored for dynamic IoT environments.

Synthesized findings were organized into conceptual categories detailing the technological synergy of federated learning and edge computing in IoT anomaly detection. Cross-study analysis enabled triangulation of results and validation of recurring themes, supported by comparative evaluation of algorithms, privacy schemes, and architectural models.

Interpretations emphasized how federated-edge paradigms contribute to preserving user privacy by obviating raw data sharing while ensuring timely and accurate anomaly

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

detection. Trade-offs between privacy guarantees, computational overhead, and detection performance were critically appraised.

RESULTS AND DISCUSSION

Federated learning combined with edge computing represents a paradigm shift for IoT anomaly detection that balances the trade-offs between centralized and fully distributed approaches. This synergy allows model training across distributed IoT devices to be achieved without sharing raw data, thus ensuring privacy and reducing communication overhead. Edge devices perform local computations, including feature extraction and anomaly detection inference, leveraging their proximity to the data sources to enable real-time responses.

Experimental and qualitative results from multiple studies converge on several key outcomes:

1. High detection accuracy achieved by federated learning models deployed at the edge, often exceeding 95% across diverse IoT datasets.
2. Significant reduction in communication overhead compared to centralized training methods, owing to local computation and transmission of model updates instead of raw data.
3. Scalability to heterogeneous IoT environments, including devices with varying computational capabilities and network conditions.
4. Privacy preservation maintained through techniques like secure aggregation and encrypted model updates.
5. Practical challenges remain in managing device heterogeneity, non-IID data distributions, and optimizing communication protocols for latency-sensitive scenarios.

The following subsections elaborate these points with qualitative data extracted from seminal studies and synthesized into tables to highlight comparative insights.

Numerous studies report that federated learning frameworks integrated with edge computing achieve high anomaly detection accuracy while preserving privacy. For example, the study published in the International Journal of Computational and Experimental Science and Engineering demonstrated detection accuracies above 96% on network traffic anomaly datasets using federated learning models combined with lightweight edge anomaly detectors.

A notable example is the FLiForest framework, which integrates federated learning with the isolation forest algorithm, yielding promising results in decentralized IoT anomaly detection scenarios with accuracy ranging from 93% to 97% across heterogeneous devices. Furthermore, hybrid deep belief network models tailored for federated learning have reached detection rates nearing 98%, as reported in recent literature.

Detection accuracy is often complemented by metrics such as low false positive rates and rapid detection times, enabling real-time alerting critical for IoT security..

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Table 1. Qualitative performance metrics

Study/Framework	Detection Accuracy (%)	False Positive Rate (%)	Detection Latency	Dataset Type	Notes
IJCESEN Federated ML	96.5	3.2	<1 second	Network Traffic	Lightweight edge-based anomaly detection
FLiForest	93 – 97	2.8	~1 second	IoT Sensor Network	Decentralized, isolation forest based
Hybrid FL Deep Belief	98.2	1.9	<1 second	Time-series IoT	Feature optimization and hyperparameter tuning
ECADA (Edge Computing)	95.1	4.0	<1.5 seconds	Industrial IoT	Lightweight algorithm suited for edge

One of the fundamental benefits of federated learning at the edge is the reduction of communication overhead, a critical factor in IoT networks where bandwidth is often constrained. Instead of transmitting voluminous raw data, IoT devices share only trained model parameters or gradients, significantly reducing data transfer size and energy consumption.

Studies highlight communication savings of up to 60%-80% compared to centralized approaches, depending on model complexity and update frequency. Techniques such as model compression, quantization, and selective update strategies further enhance bandwidth efficiency without deteriorating model accuracy.

Hierarchical federated learning architectures employing multiple aggregation layers (edge servers and cloud) optimize scalability, allowing thousands of IoT devices to collaboratively train models while mitigating latency and network congestion.

Table 2. Qualitative insights into communication overhead and scalability aspects.

Study/Framework	Communication Reduction (%)	Scalability (Devices)	Aggregation Architecture	Bandwidth Optimization Techniques
IJCESEN Federated ML	65	Up to 1000	Centralized Aggregation	Model update compression, sparse updates
FLiForest	60	500+	Single-level Federation	Feature-level pruning, selective updates
Hierarchical FL	75	10000+	Multi-layer aggregation	Layer-wise update scheduling

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Study/Framework	Communication Reduction (%)	Scalability (Devices)	Aggregation Architecture	Bandwidth Optimization Techniques
ECADA (Edge Computing)	70	Few hundreds	Edge-localized processing	Lightweight anomaly detection, asynchronous updates

Federated learning inherently enhances privacy by retaining raw data on local devices, but further safeguards are necessary to withstand inference and poisoning attacks on model updates. Several reviewed works incorporate privacy-enhancing methods such as secure multiparty computation (SMPC), homomorphic encryption (HE), differential privacy (DP), and secure aggregation protocols.

For instance, the integration of homomorphic encryption with federated learning ensures that model updates are encrypted end-to-end, making them unintelligible to aggregators while still allowing aggregation. Differential privacy mechanisms inject noise to model updates, protecting against membership inference without substantially degrading model accuracy.

Qualitative results indicate that these cryptographic and privacy-preserving measures introduce limited computational overhead manageable by most edge devices, particularly when combined with lightweight anomaly detection algorithms.

Table 3. Privacy techniques with comments on their impacts

Privacy Technique	Impact on Privacy	Computational Overhead	Effect on Model Accuracy	Applicability at Edge
Secure Aggregation	High	Low	Minimal	Suitable for resource-constrained devices
Homomorphic Encryption	Very High	Moderate	Slight	Requires careful optimization
Differential Privacy	High	Low to Moderate	Slight to Moderate	Effective trade-off with privacy
Secure MPC	Very High	High	Minimal	May limit deployment to powerful edge nodes

A persistent challenge in federated learning for IoT is the heterogeneity of device capabilities and the non-independent identically distributed (non-IID) nature of data. Different IoT devices produce data varying in volume, distribution, and quality, causing convergence difficulties and model bias.

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Many studies propose adaptive client selection strategies, weighted aggregation methods, and personalized federated learning to mitigate these issues. Adversarial federated learning techniques also enhance robustness against biased or corrupted model updates.

Qualitative analyses reveal that hierarchical federated architectures, where edge servers coordinate groups of similar devices, help balance computation loads and reduce the impact of data heterogeneity, improving convergence speeds and model generalizability.

Real-time detection capability is critical in many IoT applications such as industrial control and healthcare monitoring. Edge computing complements federated learning by enabling local inference with low latency, often below one second, facilitating timely threat mitigation.

Several studies confirm that lightweight anomaly detection algorithms, combined with asynchronous and incremental federated training, maintain high detection accuracy with minimal delay. The decentralization avoids bottlenecks and single points of failure present in cloud-centric systems. Typically, detection latencies below one second are achievable for many attack scenarios, satisfying real-time constraints.

Table 4. Qualitative attributes observed

Attribute	Observations	Challenges Addressed	Remaining Limitations
Detection Accuracy	93%–98% accuracy with low false positives	High precision in anomaly identification	Slight drops with heavy privacy protections
Communication Efficiency	Up to 75% communication reduction	Bandwidth & energy constraints	Trade-offs in update frequency
Privacy Preservation	Multi-layer cryptography and DP techniques employed	Data confidentiality & protection	Computational overhead on constrained nodes
Device and Data Heterogeneity	Adaptive aggregation, hierarchical schemes, personalized FL	Non-IID data and device variability	Complex client scheduling
Real-Time Responsiveness	Latencies <1 second in local inference & asynchronous updates	Immediate anomaly detection	Edge device resource limitations

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Attribute	Observations	Challenges Addressed	Remaining Limitations
Scalability	Systems scale to thousands of devices with hierarchical FL	Large IoT ecosystems	Synchronization challenges

The combination of FL and EC fundamentally reshapes how anomaly detection systems can be architected for IoT networks. Traditional centralized approaches, which rely on gathering raw data into cloud servers, are often impractical or unsafe due to high latency, bandwidth constraints, and serious privacy risks. The decentralized nature of federated learning, where raw data remains local and only model updates are shared, substantially mitigates privacy concerns while preserving collaborative training benefits. Edge computing complements this by enabling localized, near-source data processing that reduces the time lag between anomaly occurrence and detection (Asiri et al., 2025).

This dual paradigm empowers real-time anomaly detection with strong privacy guarantees, scalable model training, and efficient resource utilization. The results show that FL-EC systems can achieve detection accuracies nearing or exceeding 95% while managing communication overhead and resource limitations inherent in IoT deployments. These findings confirm that privacy preservation does not necessarily compromise detection performance. Instead, FL coupled with EC creates a viable operational model that balances privacy, accuracy, and latency, which is critical for practical IoT security (Eman Shalabi, 2025).

One of the central technical hurdles highlighted in the literature is the heterogeneity of IoT devices and the non-independent and identically distributed (non-IID) nature of their data. Devices vary widely in computational power, communication capabilities, and data quality. Moreover, the diversity in sensor types and deployment conditions leads to highly skewed or unbalanced data patterns that challenge the convergence and generalizability of federated models (Kais et al., 2023).

Adaptive FL algorithms that incorporate weighted aggregation, personalized federated learning, and hierarchical federated architectures have been proposed to tackle these obstacles. Hierarchical designs that impose intermediate aggregation at edge servers effectively cluster similar devices, reducing divergence caused by extreme heterogeneity and improving training stability. Similarly, personalized FL aims to tailor models to local data distributions while still benefiting from global training, enhancing detection accuracy on diverse IoT nodes (H. Yan et al., 2025).

Managing non-IID data also requires ongoing research into client selection strategies, data augmentation techniques, and synthetic anomaly data generation to compensate for label scarcity and imbalance. These approaches must harmonize with privacy requirements and minimize additional communication or computational overhead, which remains an unresolved area in many existing works (Bae et al., 2025).

The communication cost associated with federated learning remains a critical bottleneck in large-scale IoT deployments. Although FL reduces raw data transmission,

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

frequent and potentially voluminous model updates can strain limited bandwidth and energy resources, particularly in wireless or battery-powered devices (Q. Yan et al., 2025).

The research reviewed demonstrates that substantial communication savings—often exceeding 60% compared to centralized approaches—are achievable through techniques like gradient/model compression, quantization, selective update schemes, and asynchronous aggregation. Hierarchical federated learning architectures that decentralize aggregation tasks across multiple edge layers also significantly enhance scalability, allowing thousands to millions of devices to participate with manageable communication overhead (S & K R, 2025).

However, careful tuning of update frequency and aggregation intervals is vital to balancing communication cost and detection responsiveness. Latency requirements in real-time anomaly detection necessitate timely model updates to reflect evolving threat landscapes, which sometimes conflicts with minimizing network congestion. Ongoing work in dynamic, context-aware communication protocols and adaptive federated scheduling is essential to resolve these trade-offs effectively.

While federated learning inherently reduces privacy risks by keeping raw data on devices, model updates still carry potential risks of information leakage through inference or poisoning attacks. Accordingly, privacy-enhancing technologies such as secure multiparty computation (SMPC), homomorphic encryption (HE), and differential privacy (DP) are increasingly integrated into FL frameworks (Tawfik et al., 2025).

The qualitative results suggest these techniques provide robust protection with overheads that are becoming manageable for many edge devices, especially when combined with lightweight anomaly detection algorithms. For instance, secure aggregation protocols enable encrypted parameter aggregation without revealing individual updates, and differential privacy adds controlled noise to shield user data at the cost of slight accuracy loss (Zhang et al., 2025).

Nevertheless, the computation and energy demands of cryptographic operations pose practical challenges for severely resource-limited IoT nodes. Trade-offs between privacy strength, system latency, and resource consumption are critical design considerations. Future research should continue optimizing cryptographic schemes for IoT-class hardware, exploring hardware acceleration, and developing adaptive privacy budgets that reflect contextual threat levels and device capabilities (Ibrahim & Gebali, 2024).

Timeliness is paramount in IoT anomaly detection to prevent or mitigate security breaches and operational failures. Edge computing's capability to process data locally allows for near-instant anomaly detection, often achieving sub-second latencies as reported in multiple studies. Combined with asynchronous and incremental federated learning updates, systems can adapt detection models on-the-fly without blocking inference processes on devices.

This infrastructure supports timely alerts and automated responses essential for critical applications such as industrial control systems, healthcare monitoring, and autonomous vehicles. However, maintaining real-time performance requires carefully designed light detection models compatible with edge hardware constraints and efficient communication schemes that do not cause bottlenecks.

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

System designers must also consider the trade-offs between model complexity and inference latency, possibly leveraging model compression, pruning, or hybrid detection pipelines that combine lightweight detectors running continuously with heavier models updated less frequently. Proper monitoring and fallback mechanisms to handle model drift or network disruptions further enhance robustness in real-world scenarios.

CONCLUSION

This qualitative analysis highlights the substantial promise and current challenges of leveraging federated learning combined with edge computing for privacy-preserving, real-time anomaly detection in heterogeneous IoT networks. The synergy between decentralized collaborative model training and localized data processing delivers critical benefits in latency reduction, privacy protection, and scalability. Yet, addressing device heterogeneity, communication efficiency, resource constraints, and security vulnerabilities remains an ongoing research imperative. Emerging techniques in hybrid learning, adversarial defense, and hardware acceleration, coupled with ethical and regulatory awareness, are paving the way for resilient, trustworthy, and high-performance anomaly detection systems that can safeguard the pervasive IoT fabric of modern society..

REFERENCE

Alasbali, N., Ahmad, J., Siddique, A. A., Saidani, O., Al Mazroa, A., Raza, A., Ullah, R., & Khan, M. S. (2025). Privacy-enhanced skin disease classification: integrating federated learning in an IoT-enabled edge computing. *Frontiers in Computer Science*, *7*. https://doi.org/10.3389/fcomp.2025.1550677

Asiri, F., Malwi, W. Al, Masood, F., Alshehri, M. S., Zhukabayeva, T., Shah, S. A., & Ahmad, J. (2025). Privacy Preserving Federated Anomaly Detection in IoT Edge Computing Using Bayesian Game Reinforcement Learning. *Computers, Materials & Continua*, *84*(2), 3943–3960. https://doi.org/10.32604/cmc.2025.066498

Bae, W. D., Alkobaisi, S., Horak, M., Bankar, S., Bhuvaji, S., Kim, S., & Park, C.-S. (2025). Synthetic Data Generation and Evaluation Techniques for Classifiers in Data Starved Medical Applications. *IEEE Access*, *13*, 16584–16602. https://doi.org/10.1109/ACCESS.2025.3532222

Eman Shalabi. (2025). A Survey of Federated Learning Privacy Preservation Techniques for Malicious Behavior Detection. *Journal of Information Systems Engineering and Management*, *10*(51s), 659–667. https://doi.org/10.52783/jisem.v10i51s.10438

Ibrahim, A., & Gebali, F. (2024). Enhancing Field Multiplication in IoT Nodes with Limited Resources: A Low-Complexity Systolic Array Solution. *Applied Sciences*, *14*(10), 4085. https://doi.org/10.3390/app14104085

Kais, S., Bhatia, A., & Alam, M. (2023). *Quantum federated learning in healthcare: The shift from development to deployment and from models to data*. https://doi.org/10.21203/rs.3.rs-2723753/v1

Mahesh Kolli. (2025). IoT-Enabled Cybersecurity for Datacenters - Real-Time Threat Monitoring and Incident Response. *International Journal of Scientific Research in*

Computer Science, Engineering and Information Technology, *11*(2), 739–746. https://doi.org/10.32628/CSEIT25112412

Mughal, F. R., He, J., Das, B., Dharejo, F. A., Zhu, N., Khan, S. B., & Alzahrani, S. (2024). Adaptive federated learning for resource-constrained IoT devices through edge intelligence and multi-edge clustering. *Scientific Reports*, *14*(1), 28746. https://doi.org/10.1038/s41598-024-78239-z

Odeh, J. O., Yang, X., Samuel, O. W., Dhelim, S., & Nwakanma, C. I. (2025). Systematic investigation of privacy preservation techniques for industrial IoT-enabled critical edge network Infrastructure. *Cluster Computing*, *28*(6), 407. https://doi.org/10.1007/s10586-025-05114-5

S, M., & K R, J. (2025). Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management. *Scientific Reports*, *15*(1), 27524. https://doi.org/10.1038/s41598-025-12225-x

Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. *Cluster Computing*, *28*(3), 191. https://doi.org/10.1007/s10586-024-04928-z

Tiwari, P. S., Pali, P. P., Patel, P. A., Pasi, J., & Jain, M. (2023). Optimizing Data Processing and Security in Edge Computing For Iot Applications. *International Journal of Innovative Research in Science,Engineering and Technology*, *12*(05), 8040–8043. https://doi.org/10.15680/IJIRSET.2023.1205494

Yan, H., Lin, X., Li, S., Peng, H., & Zhang, B. (2025). Global or Local Adaptation? Client-Sampled Federated Meta-Learning for Personalized IoT Intrusion Detection. *IEEE Transactions on Information Forensics and Security*, *20*, 279–293. https://doi.org/10.1109/TIFS.2024.3516548

Yan, Q., Wang, G., Zhu, D., & Li, J. (2025). FedIoT: Optimizing the Communication-Efficient Federated Learning Aggregation Algorithm Under Heterogeneous Data for Large-Scale IoT. *International Journal of Pattern Recognition and Artificial Intelligence*, *39*(11). https://doi.org/10.1142/S0218001425520135

Zhang, Y., Behnia, R., Yavuz, A. A., Ebrahimi, R., & Bertino, E. (2025). Efficient Full-Stack Private Federated Deep Learning with Post-Quantum Security. *IEEE Transactions on Dependable and Secure Computing*, 1–17. https://doi.org/10.1109/TDSC.2025.3568704