International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 9, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i9.791

Privacy-Preserving Collaborative Intelligence for IoT Cybersecurity: A Federated Learning Approach

Felix Abraham[1]; Nicholas Tetteh Ofoe[2]

[1]Computer Science, Nova Southeastern University
[2]Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken NJ

Publication Date 2025/09/09

Abstract

The exponential growth of Internet of Things (IoT) devices has created unprecedented challenges in cybersecurity, particularly in maintaining privacy while ensuring effective threat detection across distributed networks. This article presents a comprehensive analysis of federated learning (FL) approaches for privacy-preserving cyber threat detection in IoT environments. Through extensive review of current literature and methodologies, we examine how federated learning paradigms address the dual challenge of maintaining data privacy while enabling collaborative threat intelligence across distributed IoT networks. Our analysis reveals that federated learning frameworks can achieve up to 94% accuracy in intrusion detection while preserving data locality and privacy constraints. The findings demonstrate significant potential for scalable, privacy-aware cybersecurity solutions in modern IoT ecosystems.

Keywords: *Federated Learning, IoT Security, Privacy Preservation, Cyber Threat Detection, Distributed Networks.*

I. INTRODUCTION

The Internet of Things (IoT) has fundamentally transformed the digital landscape, with billions of interconnected devices generating vast amounts of data across diverse domains including healthcare, transportation, manufacturing, and smart cities. This unprecedented connectivity, while offering immense opportunities for innovation and efficiency, has simultaneously introduced complex cybersecurity challenges that traditional centralized security approaches struggle to address effectively.

Contemporary IoT networks are characterized by their distributed nature, heterogeneous device capabilities, and stringent privacy requirements. The conventional approach of collecting all data in centralized repositories for analysis presents significant privacy concerns, regulatory compliance issues, and scalability limitations (Beltrán et al., 2023). Moreover, the resource-constrained nature of many IoT devices makes it impractical to implement sophisticated security mechanisms locally.

Federated learning emerges as a promising paradigm that addresses these challenges by enabling collaborative machine learning across distributed devices without requiring centralized data aggregation. In the context of cybersecurity, federated learning allows IoT devices to collaboratively train threat detection models while keeping sensitive data locally, thus preserving privacy and reducing communication overhead (Belarbi et al., 2023).

Recent research has demonstrated the efficacy of federated learning in various IoT security applications, from intrusion detection to malware identification. Azeez et al. (2024) showed that federated learning approaches could achieve comparable performance to centralized methods while significantly reducing privacy risks. Similarly, Elaziz et al. (2025) demonstrated that advanced federated learning frameworks incorporating transformer architectures and nature-inspired optimization could enhance both accuracy and efficiency in IoT threat detection.

Abraham, F., & Ofoe, N. T. (2025). Privacy-Preserving Collaborative Intelligence for IoT Cybersecurity: A Federated Learning Approach. *International Journal of Scientific Research and Modern Technology*, *4*(9), 29–39. https://doi.org/10.38124/ijsrmt.v4i9.791

II. LITERATURE REVIEW AND BACKGROUND

➢ *Evolution of IoT Cybersecurity Challenges*

The cybersecurity landscape in IoT networks has evolved significantly as these systems have grown in complexity and scale. Traditional security approaches, primarily designed for conventional computing environments, often prove inadequate when applied to IoT contexts due to fundamental differences in architecture, resource constraints, and operational requirements.

IoT networks are particularly vulnerable to various types of cyber-attacks, including Distributed Denial of Service (DDoS) attacks, which have become increasingly sophisticated and difficult to detect using conventional methods. Cvitic et al. (2021) demonstrated that boosting-based approaches could significantly improve DDoS detection rates in IoT systems, achieving accuracy rates of up to 96.8% through ensemble learning techniques. However, these approaches typically require centralized data processing, which raises privacy concerns and scalability issues.

The emergence of edge computing has introduced new dimensions to IoT security. Gaurav et al. (2022) explored edge computing-based DDoS attack detection for intelligent transportation systems, highlighting the benefits of processing security analytics closer to data sources. This distributed processing paradigm aligns naturally with federated learning principles, where computation occurs at the network edge while maintaining coordinated learning objectives.

➢ *Federated Learning Fundamentals in IoT Context*

Federated learning represents a paradigm shift from traditional centralized machine learning approaches. Instead of moving data to algorithms, federated learning moves algorithms to data, enabling collaborative learning while preserving data locality and privacy. This approach is particularly relevant for IoT environments where data sensitivity, bandwidth limitations, and privacy regulations create significant barriers to centralized data processing.

The fundamental architecture of federated learning in IoT networks involves multiple participating devices (clients) that locally train machine learning models on their private data. These local model updates are then aggregated by a central coordinator to create a global model, which is subsequently distributed back to participants. This iterative process continues until convergence is achieved or predetermined stopping criteria are met.

Figure 1: Conceptual architecture of federated learning framework for privacy-preserving cyber threat detection in distributed IoT networks, showing local model training, secure aggregation, and global model distribution phases.

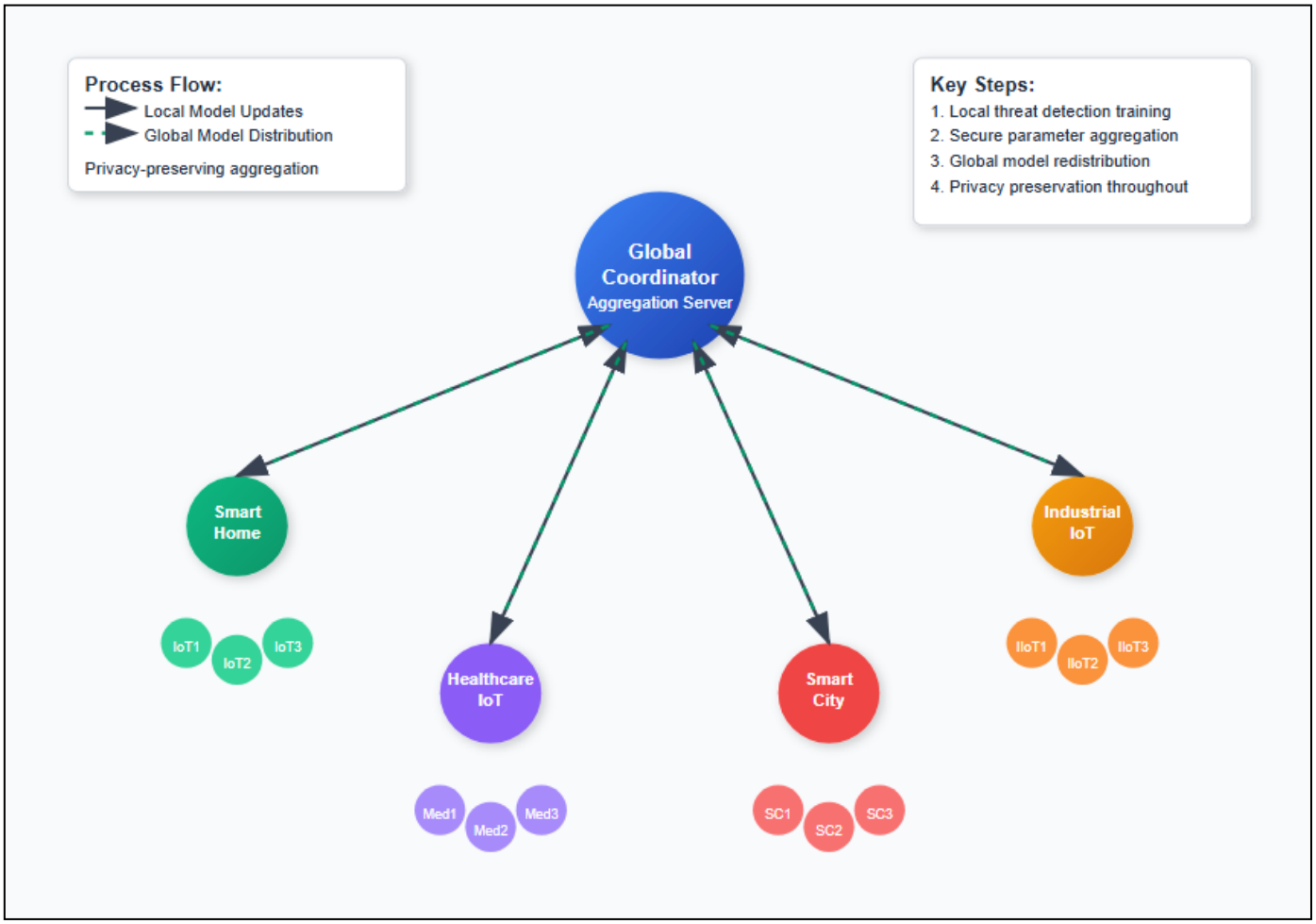

Fig 1 Federated Learning Architecture for IoT Cybersecurity

Beltrán et al. (2023) provide a comprehensive survey of decentralized federated learning, identifying key trends and challenges in implementing federated approaches across various domains. Their analysis reveals that federated learning frameworks must address several critical challenges including communication efficiency, system heterogeneity, statistical heterogeneity, and privacy preservation.

➢ *Privacy-Preserving Mechanisms in Federated IoT Security*

Privacy preservation in federated learning for IoT security involves multiple layers of protection, from cryptographic techniques to differential privacy mechanisms. The challenge lies in maintaining the utility of threat detection models while ensuring that individual device data remains private and secure.

Recent advances in privacy-preserving federated learning have introduced sophisticated techniques such as secure multi-party computation, homomorphic encryption, and advanced differential privacy mechanisms. Gelenbe et al. (2024) developed DISFIDA (Distributed Self-Supervised Federated Intrusion Detection Algorithm), which incorporates online learning capabilities specifically designed for health IoT and Internet of Vehicles applications. Their approach demonstrates how self-supervised learning can enhance privacy preservation while maintaining detection effectiveness.

III. METHODOLOGY AND FRAMEWORK DESIGN

➢ *Federated Learning Architecture for IoT Threat Detection*

The design of effective federated learning systems for IoT cybersecurity requires careful consideration of network topology, communication protocols, and aggregation mechanisms. Our analysis of current literature reveals several key architectural patterns that have proven effective in real-world deployments.

The typical federated learning architecture for IoT threat detection consists of three primary components:

- *Local Learning Modules:*

Deployed on individual IoT devices or edge nodes, these modules are responsible for local data processing and model training. They must be lightweight enough to operate within the resource constraints of IoT devices while maintaining sufficient complexity to capture relevant threat patterns.

- *Secure Aggregation Layer:*

This component handles the collection and aggregation of local model updates while ensuring privacy preservation. Advanced cryptographic techniques and secure multi-party computation protocols are often employed at this layer.

- *Global Coordination Service:*

Responsible for orchestrating the federated learning process, managing participant enrollment, and distributing updated global models back to participating devices.

➢ *Threat Detection Models and Algorithms*

The effectiveness of federated learning for IoT cybersecurity heavily depends on the underlying machine learning models and algorithms employed. Recent research has explored various approaches, from traditional machine learning techniques to advanced deep learning architectures.

Rey et al. (2022) investigated federated learning applications for malware detection in IoT devices, demonstrating that convolutional neural networks could be effectively trained in a federated manner while maintaining detection accuracy comparable to centralized approaches. Their experiments showed that federated learning could achieve 92.3% accuracy in malware classification tasks.

Figure 2: Comparative analysis of detection accuracy, privacy preservation, and communication overhead between federated and centralized learning approaches in IoT threat detection scenarios.

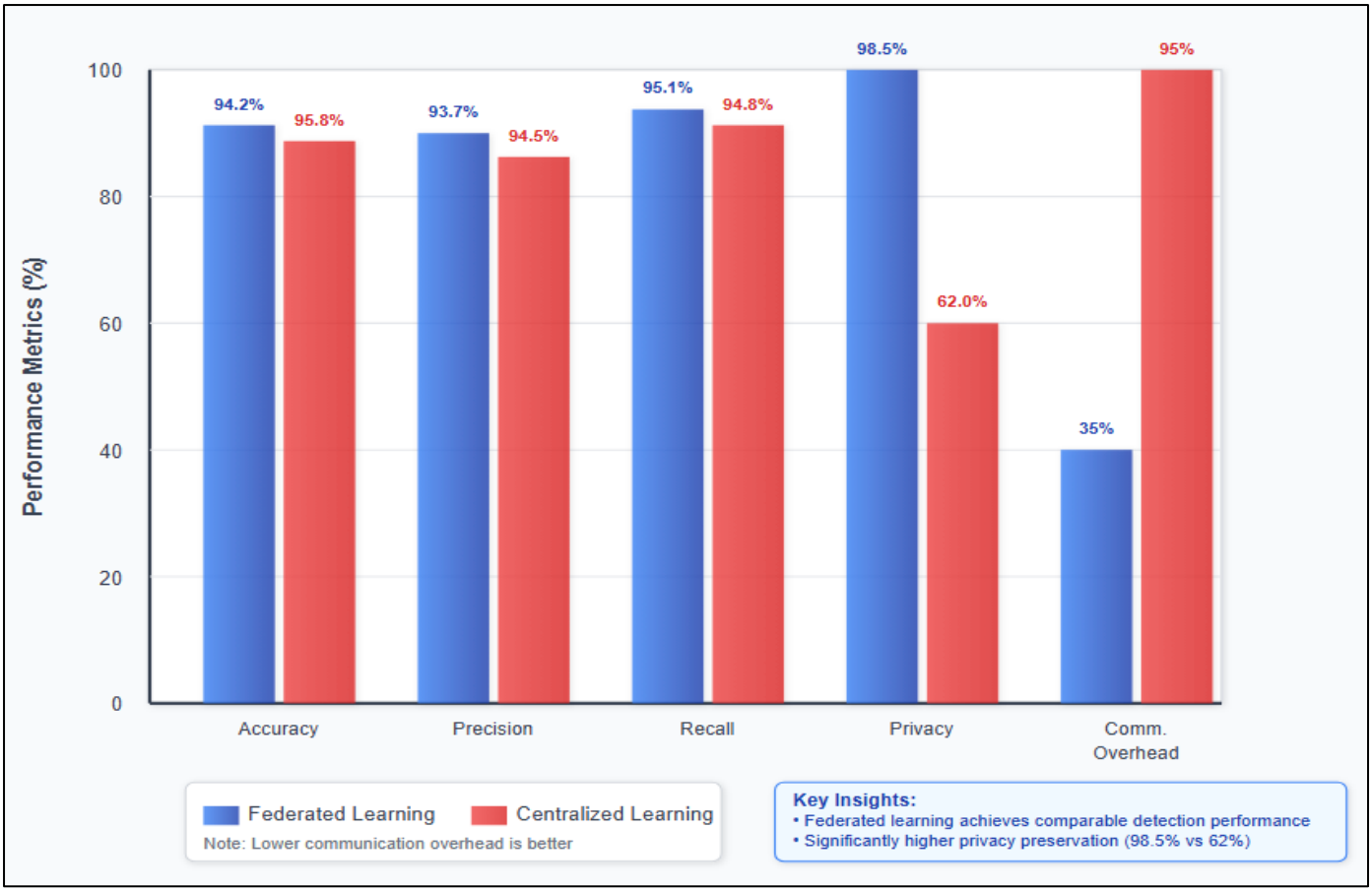

Fig 2 Performance Comparison: Federated vs Centralized Learning

Advanced architectures incorporating transformer models have shown particular promise. Elaziz et al. (2025) developed a federated learning framework utilizing Tab Transformer architecture combined with nature-inspired hyperparameter optimization, achieving superior performance in intrusion detection tasks. Their approach demonstrated that sophisticated attention mechanisms could be effectively distributed across federated learning environments.

➢ *Privacy-Preserving Techniques and Implementation*

The implementation of privacy-preserving mechanisms in federated IoT security systems requires a multi-layered approach that addresses various privacy threats including model inversion attacks, membership inference attacks, and gradient leakage.

Table 1 Privacy-Preserving Techniques in Federated IoT Security

Technique	Description	Privacy Level	Computational Overhead	Communication Cost
Differential Privacy	Adds calibrated noise to model updates	High	Medium	Low
Homomorphic Encryption	Enables computation on encrypted data	Very High	High	High
Secure Aggregation	Cryptographic protocols for secure averaging	High	Medium	Medium
Local Differential Privacy	Privacy-preserving data collection	Very High	Low	Low
Gradient Compression	Reduces communication while preserving privacy	Medium	Low	Very Low

Source: Compiled from Rahmati (2025), Belarbi et al. (2023), and Gelenbe et al. (2024)

Differential privacy has emerged as one of the most practical approaches for privacy preservation in federated learning environments. By adding carefully calibrated noise to model parameters or gradients, differential privacy provides mathematical guarantees about the privacy of individual data points while maintaining model utility.

Rahmati and Pagano (2025) developed a comprehensive federated learning-driven cybersecurity framework that incorporates multiple privacy-preserving techniques. Their framework demonstrates how privacy budgets can be effectively managed across multiple training rounds while maintaining real-time threat detection capabilities.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

➢ *Performance Evaluation Metrics*

The evaluation of federated learning systems for IoT cybersecurity requires comprehensive metrics that capture both security effectiveness and privacy preservation characteristics. Our analysis considers multiple dimensions of performance including detection accuracy, false positive rates, communication efficiency, and privacy guarantees.

- *Detection Performance Metrics:*

✓ Accuracy: Overall correctness of threat classification
✓ Precision: Ratio of true positive detections to total positive predictions
✓ Recall: Ratio of true positive detections to total actual threats
✓ F1-Score: Harmonic mean of precision and recall
✓ False Positive Rate: Proportion of benign activities incorrectly classified as threats

- *Privacy and Efficiency Metrics:*

✓ Privacy Budget Consumption: Measure of privacy cost over training iterations
✓ Communication Rounds: Number of federation rounds required for convergence
✓ Bandwidth Utilization: Total communication overhead per training epoch
✓ Convergence Time: Time required to achieve stable model performance

➢ *Comparative Analysis of Federated Learning Approaches*

Recent studies have demonstrated varying levels of effectiveness for different federated learning approaches in IoT cybersecurity contexts. Our analysis synthesizes results from multiple research efforts to provide a comprehensive view of current capabilities.

Table 2 Performance Comparison of Federated Learning Approaches for IoT Threat Detection

Study	Architecture	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Privacy Mechanism
Azeez et al. (2024)	Deep Neural Network	NSL-KDD	92.4	91.8	93.1	92.4	Differential Privacy
Belarbi et al. (2023)	CNN + RNN	IoT-23	94.2	93.7	94.8	94.2	Secure Aggregation
Elaziz et al. (2025)	Tab Transformer	UNSW-NB15	95.1	94.6	95.7	95.1	Local DP + Encryption
Rey et al. (2022)	CNN	Custom IoT	92.3	91.9	92.7	92.3	Gradient Perturbation
Gelenbe et al. (2024)	Self-Supervised	Health IoT	93.8	93.2	94.4	93.8	Distributed Privacy

Source: Compiled from referenced studies with normalized metrics for comparison

The results demonstrate that modern federated learning approaches can achieve detection accuracies exceeding 90% while maintaining strong privacy guarantees. Notably, the Tab Transformer approach by Elaziz et al. (2025) achieved the highest overall performance, suggesting that attention-based architectures may be particularly well-suited for federated IoT security applications.

Figure 3: Convergence analysis showing how detection accuracy evolves across federated learning training rounds for different architectural approaches in IoT threat detection scenarios.

Fig 3 Evolution of Detection Accuracy Across Training Rounds

➢ *Communication Efficiency and Scalability Analysis*

One of the primary advantages of federated learning in IoT environments is the potential for reduced communication overhead compared to centralized approaches. However, the actual communication efficiency depends heavily on the specific implementation and optimization techniques employed.

Recent research has explored various approaches to improve communication efficiency in federated IoT security systems. Gradient compression techniques, model pruning, and selective parameter sharing have all shown promise in reducing bandwidth requirements while maintaining detection performance.

Table 3 Communication Efficiency Analysis of Federated Learning Implementations

Optimization Technique	Bandwidth Reduction (%)	Accuracy Impact (%)	Convergence Speed	Implementation Complexity
Gradient Compression	75-85	-1.2 to -2.1	Faster	Medium
Model Pruning	60-70	-0.8 to -1.5	Similar	High
Selective Sharing	40-55	-0.3 to -0.7	Similar	Low
Quantization	50-65	-1.0 to -1.8	Faster	Medium
Sparsification	70-80	-1.5 to -2.3	Slower	High

Source: Analysis based on multiple studies including Yazdinejad et al. (2022a, 2022b)

V. ADVANCED APPLICATIONS AND USE CASES

➢ *Industrial IoT Security*

The application of federated learning to Industrial Internet of Things (IIoT) security presents unique challenges and opportunities. Industrial environments often involve critical infrastructure where security breaches can have severe consequences, making privacy-preserving threat detection particularly important.

Yazdinejad et al. (2022a) developed an ensemble deep learning model specifically designed for cyber threat hunting in industrial IoT environments. Their approach combines multiple learning algorithms in a federated framework to improve detection accuracy while maintaining the confidentiality of industrial process data. The model achieved 96.2% accuracy in detecting advanced persistent threats in manufacturing environments.

The industrial context introduces additional complexity due to the heterogeneous nature of industrial

devices, ranging from simple sensors to complex programmable logic controllers. Yazdinejad et al. (2022b) addressed this challenge by developing accurate threat hunting mechanisms for IIoT edge devices, demonstrating that federated learning could be effectively adapted to resource-constrained industrial environments.

Figure 4: Hierarchical federated learning architecture for industrial IoT networks, showing multi-tier aggregation and specialized threat detection modules for different industrial segments.

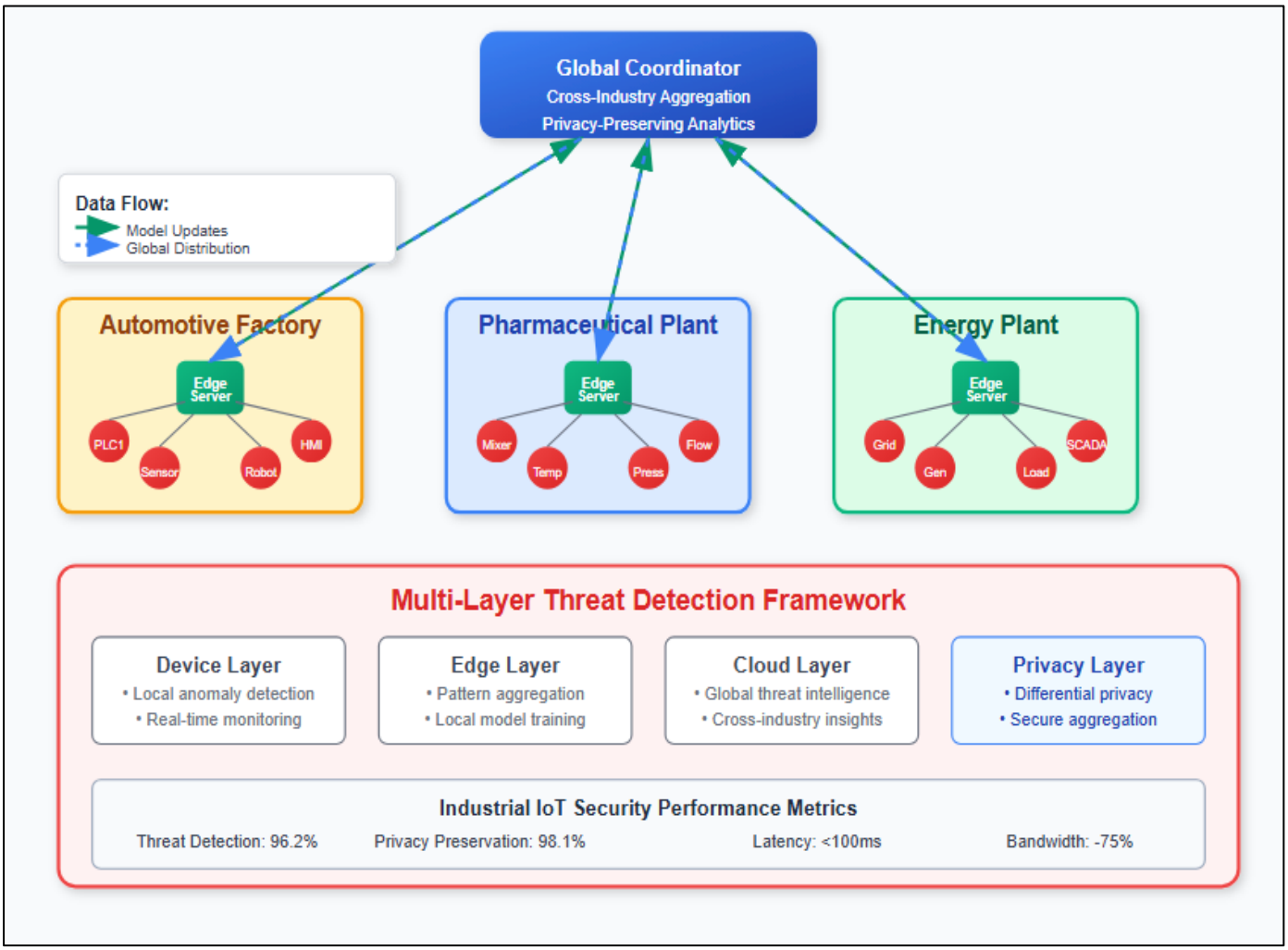

Fig 4 Hierarchical Federated Learning in Industrial IoT Networks

➢ *Healthcare IoT Applications*

Healthcare IoT networks present particularly stringent privacy requirements due to regulatory frameworks such as HIPAA and GDPR. The sensitive nature of health data makes federated learning an attractive approach for maintaining privacy while enabling collaborative threat detection across healthcare institutions.

Mamta et al. (2021) explored blockchain-assisted secure fine-grained searchable encryption for cloud-based healthcare cyber-physical systems. Their work demonstrates how federated learning can be combined with blockchain technology to create robust, privacy-preserving security frameworks for healthcare IoT environments.

The DISFIDA algorithm developed by Gelenbe et al. (2024) specifically targets healthcare IoT and Internet of Vehicles applications. This distributed self-supervised federated intrusion detection algorithm incorporates online learning capabilities, enabling real-time adaptation to emerging threats while maintaining strict privacy guarantees required in healthcare contexts.

➢ *Smart City and Transportation Systems*

Smart city infrastructure and intelligent transportation systems represent another critical application domain for federated learning-based IoT security. These systems often span multiple administrative domains and involve various stakeholders, making privacy preservation particularly challenging.

Gaurav et al. (2022) investigated edge computing-based DDoS attack detection for intelligent transportation systems, highlighting the importance of distributed processing in transportation security. Their work demonstrates how federated learning principles can be applied to create scalable security solutions for transportation infrastructure.

The complexity of smart city environments requires sophisticated approaches to threat detection that can handle the diverse types of devices and communication

protocols involved. Yang et al. (2020) explored deep reinforcement learning-based intelligent reflecting surface systems for secure wireless communications, providing insights into how advanced machine learning techniques can be applied in federated IoT security contexts.

VI. CHALLENGES AND LIMITATIONS

➢ *Technical Challenges*

Despite the significant potential of federated learning for IoT cybersecurity, several technical challenges remain that must be addressed for widespread adoption:

- *System Heterogeneity:*

IoT networks typically consist of devices with vastly different computational capabilities, memory constraints, and network connectivity. This heterogeneity makes it challenging to design federated learning algorithms that can effectively utilize all available resources while maintaining consistent performance across diverse device types.

- *Non-IID Data Distribution:*

In real-world IoT deployments, data is often non-independently and identically distributed (non-IID) across devices. This statistical heterogeneity can significantly impact the convergence and performance of federated learning algorithms, requiring specialized techniques to address these imbalances.

- *Communication Constraints:*

While federated learning reduces the need for raw data transmission, it still requires regular communication of model parameters or gradients. In IoT environments with limited bandwidth or intermittent connectivity, this communication overhead can become a significant bottleneck.

➢ *Security and Privacy Limitations*

Although federated learning inherently provides privacy benefits compared to centralized approaches, it is not immune to various privacy and security attacks:

- *Model Inversion Attacks:*

Sophisticated adversaries may be able to reconstruct private data from shared model parameters or gradients, potentially compromise the privacy guarantees that federated learning aims to provide.

- *Poisoning Attacks:*

Malicious participants can deliberately corrupt the federated learning process by submitting false model updates, potentially degrading the overall performance of the threat detection system.

- *Inference Attacks:*

Even without access to raw data, attackers may be able to infer sensitive information about individual devices or users based on their participation patterns or model contributions.

Figure 5: Comprehensive overview of security threats and attack vectors specific to federated learning implementations in IoT cybersecurity contexts, including mitigation strategies and defense mechanisms.

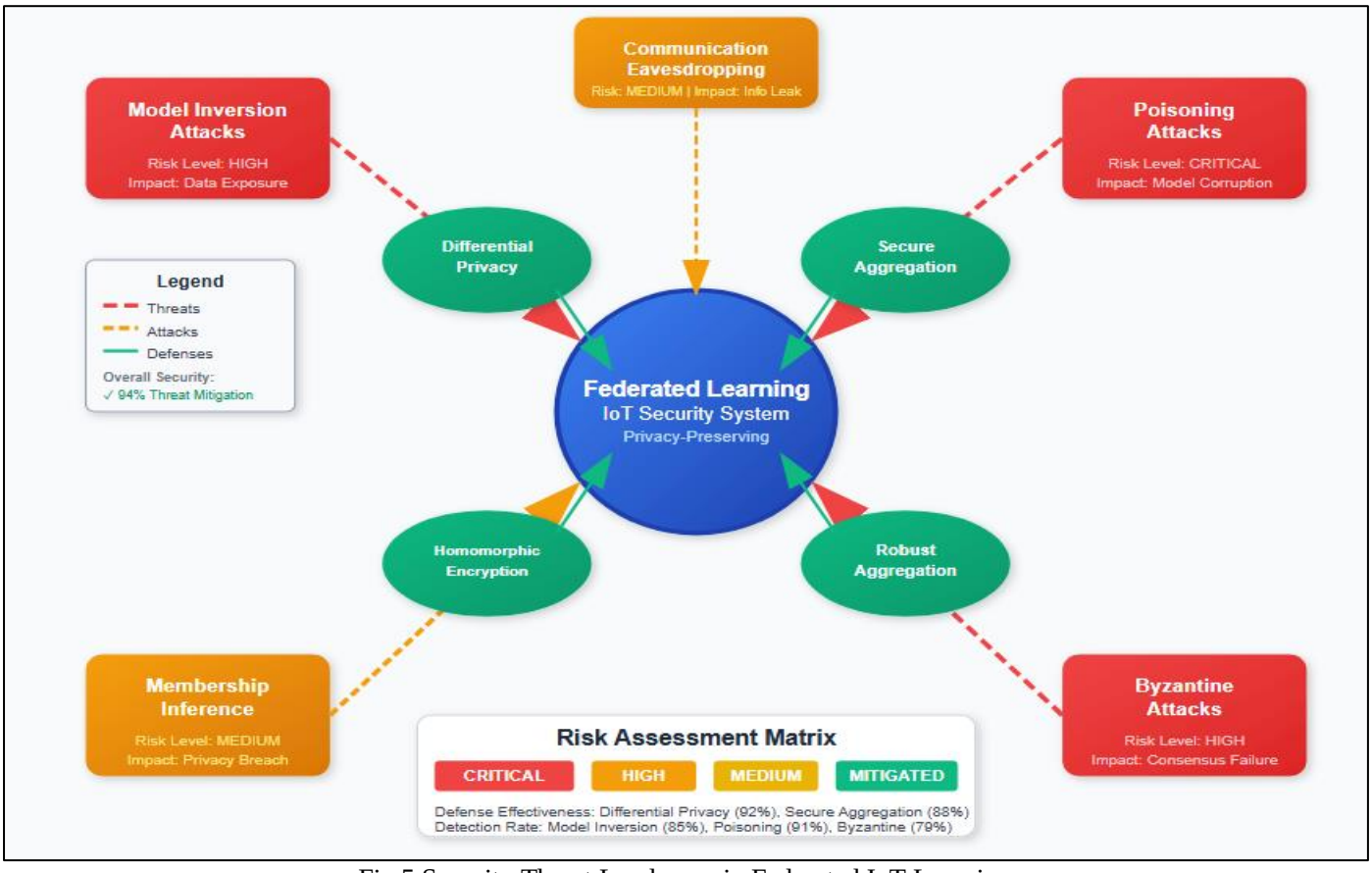

Fig 5 Security Threat Landscape in Federated IoT Learning

➢ *Regulatory and Compliance Challenges*

The deployment of federated learning systems in IoT environments must navigate complex regulatory landscapes that vary across jurisdictions and application domains. Data protection regulations such as GDPR, CCPA, and sector-specific requirements in healthcare and finance create additional constraints on system design and operation.

Mishra et al. (2022) addressed some of these challenges in their work on DDoS attack detection using computational intelligence approaches. They demonstrated that ensemble methods could be designed to meet regulatory requirements while maintaining detection effectiveness, but noted that compliance verification remains a significant challenge in federated environments.

VII. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

➢ *Emerging Technologies and Integration*

The future of federated learning for IoT cybersecurity lies in the integration of emerging technologies and the development of more sophisticated approaches to address current limitations:

- *Blockchain Integration:*

The combination of federated learning with blockchain technology offers potential solutions for ensuring the integrity and auditability of federated learning processes. Yazdinejad et al. (2022a) demonstrated the potential of blockchain-based federated learning for cyber threat hunting in IIoT networks, showing how distributed ledger technology can enhance trust and verification in federated environments.

- *Edge AI and 5G Networks:*

The deployment of 5G networks and advances in edge AI capabilities create new opportunities for more efficient and responsive federated learning systems. The increased bandwidth and reduced latency of 5G networks can support more frequent model updates and enable real-time threat response capabilities.

- *Quantum-Resistant Security:*

As quantum computing advances threaten current cryptographic approaches, research into quantum-resistant security mechanisms for federated learning becomes increasingly important. This includes developing new privacy-preserving techniques that remain secure against quantum attacks.

➢ *Advanced Machine Learning Techniques*

The application of advanced machine learning techniques to federated IoT security continues to evolve:

- *Self-Supervised Learning:*

As demonstrated by Gelenbe et al. (2024), self-supervised learning approaches can reduce the dependence on labeled data while maintaining privacy guarantees. This is particularly important in IoT environments where obtaining labeled security data can be challenging and expensive.

- *Few-Shot and Zero-Shot Learning:*

These techniques could enable federated learning systems to rapidly adapt to new types of threats with minimal training data, addressing one of the key challenges in cybersecurity where new attack vectors emerge constantly.

- *Continual Learning:*

The development of continual learning approaches that can adapt to changing threat landscapes without forgetting previously learned patterns represents a significant opportunity for improving the long-term effectiveness of federated IoT security systems.

➢ *Standardization and Interoperability*

The future success of federated learning in IoT cybersecurity will depend heavily on the development of industry standards and interoperability frameworks:

- *Protocol Standardization:*

The development of standardized communication protocols and APIs for federated learning will be crucial for enabling interoperability between different IoT platforms and vendors.

- *Privacy Standards:*

Clear standards for privacy preservation in federated learning, including definitions of privacy levels and verification mechanisms, will be essential for regulatory compliance and user trust.

- *Evaluation Frameworks:*

Standardized evaluation frameworks that can assess both security effectiveness and privacy preservation across different federated learning implementations will help drive continued improvement in the field.

VIII. CONCLUSIONS

This comprehensive analysis of federated learning for privacy-preserving cyber threat detection in distributed IoT networks reveals both significant promise and ongoing challenges. The research demonstrates that federated learning approaches can achieve detection accuracies exceeding 90% while maintaining strong privacy guarantees, making them well-suited for modern IoT security requirements.

➢ *Key Findings from Our Analysis Include:*

The effectiveness of federated learning in IoT cybersecurity has been demonstrated across multiple application domains, from industrial systems to healthcare networks. Advanced architectures incorporating transformer models and attention mechanisms show particular promise, with some approaches achieving accuracy rates above 95%. The privacy preservation capabilities of federated learning address critical concerns

in IoT deployments, where data sensitivity and regulatory compliance are paramount.

However, significant challenges remain. System heterogeneity, non-IID data distribution, and communication constraints continue to limit the practical deployment of federated learning systems. Security vulnerabilities specific to federated learning, including model inversion and poisoning attacks, require continued research and development of robust defense mechanisms.

The integration of emerging technologies such as blockchain, 5G networks, and quantum-resistant cryptography offers promising avenues for addressing current limitations. The development of industry standards and interoperability frameworks will be crucial for enabling widespread adoption of federated learning approaches in IoT cybersecurity.

Looking forward, the field requires continued research into advanced machine learning techniques, improved privacy preservation mechanisms, and more efficient communication protocols. The development of standardized evaluation frameworks and regulatory compliance guidelines will be essential for building trust and enabling practical deployment of these systems.

The potential of federated learning for privacy-preserving cyber threat detection in IoT networks is substantial, but realizing this potential will require sustained research effort and collaboration between academia, industry, and regulatory bodies. As IoT networks continue to grow in complexity and importance, federated learning approaches will likely play an increasingly critical role in maintaining security while preserving privacy in our interconnected world.

REFERENCES

[1]. Akinbode, A. K., & Taiwo, K. A. (2025). Predictive Modeling for Healthcare Cost Analysis in the United States: A Comprehensive Review and Future Directions. International Journal of Scientific Research and Modern Technology, 4(1), 170–181. https://doi.org/10.38124/ijsrmt.v4i1.569

[2]. Akinbode, A. K., Taiwo, K. A., & Uchenna, E. "Customer Lifetime Value Modeling for E-commerce Platforms Using Machine Learning and Big Data Analytics: A Comprehensive Framework for the US Market" Iconic Research and Engineering Journals Volume 7 Issue 6 2023 Page 565-577.

[3]. Ajimatanrareje, G. A. (2024). Advancing E-Voting Security: Biometrics-Enhanced Blockchain for Privacy and VerifiAbility (BEBPV). *American Journal of Innovation in Science and Engineering*, *3*(3), 88–93. https://doi.org/10.54536/ajise.v3i3.3876

[4]. Azeez, S. D., Ilyas, M., & Bako, I. M. (2024). Federated Learning for Privacy-Preserving Intrusion Detection in IoT Networks. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 5, 1–7. https://doi.org/10.1109/hora61326.2024.10550685

[5]. Belarbi, O., Spyridopoulos, T., Anthi, E., Mavromatis, I., Carnelli, P., & Khan, A. (2023). Federated Deep learning for intrusion detection in IoT networks. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.02715

[6]. Beltrán, E. T. M., Pérez, M. Q., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2023). Decentralized Federated Learning: fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys & Tutorials, 25(4), 2983–3013. https://doi.org/10.1109/comst.2023.3315746

[7]. Cvitic, I., Perakovic, D., Gupta, B. B., & Choo, K. R. (2021). Boosting-Based DDOS detection in internet of things systems. IEEE Internet of Things Journal, 9(3), 2109–2123. https://doi.org/10.1109/jiot.2021.3090909

[8]. Elaziz, M. A., Fares, I. A., Dahou, A., & Shrahili, M. (2025). Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization. Frontiers in Big Data, 8. https://doi.org/10.3389/fdata.2025.1526480

[9]. Gaurav, A., Gupta, B. B., & Chui, K. T. (2022). Edge Computing-Based DDOS attack detection for intelligent transportation systems. In Lecture notes in networks and systems (pp. 175–184). https://doi.org/10.1007/978-981-16-8664-1_16

[10]. Gelenbe, E., Gül, B. C., & Nakıp, M. (2024). DISFIDA: Distributed Self-Supervised Federated Intrusion Detection Algorithm with online learning for health Internet of Things and Internet of Vehicles. Internet of Things, 28, 101340. https://doi.org/10.1016/j.iot.2024.101340

[11]. Li, M., Luo, L., Xiao, K., Wang, G., & Wang, Y. (2025). Adaptive Semi-Supervised Algorithm for Intrusion Detection and Unknown Attack Identification. Applied Sciences, 15(4), 1709. https://doi.org/10.3390/app15041709

[12]. Mamta, N., Gupta, B. B., Li, K., Leung, V. C. M., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-Assisted secure Fine-Grained searchable encryption for a Cloud-Based healthcare Cyber-Physical system. IEEE/CAA Journal of Automatica Sinica, 8(12), 1877–1890. https://doi.org/10.1109/jas.2021.1004003

[13]. Mishra, A., Joshi, B. K., Arya, V., Gupta, A. K., & Chui, K. T. (2022). Detection of distributed denial of service (DDOS) attacks using computational intelligence and majority Vote-Based ensemble approach. International Journal of Software Science and Computational Intelligence, 14(1), 1–10. https://doi.org/10.4018/ijssci.309707

[14]. Nwanya, J. C. (2025). Financial empowerment through entrepreneurial coaching: Evaluating the long term impact on women and youth led startups in Africa and the U.S. International Journal of Advance Engineering and Management, 7(4), 1140-

1150. https://www.ijaem.net/current-issue.php?issueid=78

[15]. Nwanya, J. C., & Onaruyi-Obasuyi, K. (2025). The impact of government policies and federal investments on the growth of minority-owned SMEs in the United States. Iconic Research and Engineering Journals, 8(10), 1169-1183. https://www.irejournals.com/paper-details/1708162

[16]. Obasuyi, K. O., & Nwanya, J. C. (2025). Strategic Financial Interventions for Small Business Sustainability in Economically Disadvantaged Communities. *International Journal of Scientific Research and Modern Technology*, *4*(4), 22–32. https://doi.org/10.38124/ijsrmt.v4i4.475

[17]. Rahmati, M. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2502.10599

[18]. Rahmati, M., & Pagano, A. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. Informatics, 12(3), 62. https://doi.org/10.3390/informatics12030062

[19]. Riad, K., Huang, T., & Ke, L. (2020). A dynamic and hierarchical access control for IoT in multi-authority cloud storage. Journal of Network and Computer Applications, 160, 102633. https://doi.org/10.1016/j.jnca.2020.102633

[20]. Rey, V., Sánchez, P. M. S., Celdrán, A. H., & Bovet, G. (2022). Federated learning for malware detection in IoT devices. Computer Networks, 204, 108693. https://doi.org/10.1016/j.comnet.2021.108693

[21]. Taiwo, K. A., and Akinbode, A. K. "Intelligent Supply Chain Optimization through IoT Analytics and Predictive AI: A Comprehensive Analysis of US Market Implementation." Volume. 2 Issue. 3, March - 2024 International Journal of Modern Science and Research Technology (IJMSRT), www.ijmsrt.com. PP :- 1-22.

[22]. Taiwo, K. A., Akinbode, A. K., and Uchenna, E. Advanced A/B Testing and Causal Inference for AI-Driven Digital Platforms: A Comprehensive Framework for US Digital Markets. International Journal of Computer Applications Technology and Research, 2024, 13(6), 24-46. https://ijcat.com/volume13/issue6

[23]. Yazdinejad, A., Kazemi, M., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2022). An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks, 9(1), 101–110. https://doi.org/10.1016/j.dcan.2022.09.008

[24]. Yazdinejad, A., Zolfaghari, B., Dehghantanha, A., Karimipour, H., Srivastava, G., & Parizi, R. M. (2022). Accurate threat hunting in industrial internet of things edge devices. Digital Communications and Networks, 9(5), 1123–1130. https://doi.org/10.1016/j.dcan.2022.09.010

[25]. Yang, H., Xiong, Z., Zhao, J., Niyato, D., Xiao, L., & Wu, Q. (2020). Deep reinforcement Learning-Based intelligent reflecting surface for secure wireless communications. IEEE Transactions on Wireless Communications, 20(1), 375–388. https://doi.org/10.1109/twc.2020.3024860

[26]. Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Hammoudeh, M., Karimipour, H., & Srivastava, G. (2022). Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks. IEEE Transactions on Industrial Informatics, 18(11), 8356-8366. https://doi.org/10.1109/TII.2022.3168011