Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Federated Edge-to-Cloud AI Infrastructure for Adaptive Cyber Resilience

Venkata Thej Deep Jakkaraju

Cloud Architect, GameStop, Grapevine, Texas

thejdeep.j@outlook.com

Article History:
Received: 04-10-2025
Revised: 09-11-2025
Accepted: 12-12-2025

Abstract:
A rapid shift toward distributed intelligent systems at the network edge, combined with escalating cyber threats, has created a structural mismatch between traditional cloud-centric security architectures and the requirements of ultra-low-latency, privacy-preserving, and resilient operations. By 2025, approximately 75% of enterprise-generated data is expected to be created and processed outside traditional data centers, up from roughly 10% in 2019, while connected IoT devices are projected to reach about 27.1 billion globally. Global cybercrime damage is forecast to reach 10.5 trillion USD annually, and the average cost of a data breach has risen to 4.45 million USD. These dynamics motivate an integrated federated edge-to-cloud AI infrastructure in which security analytics are distributed, models are trained collaboratively without centralizing raw data, and control is enforced through zero-trust, policy-driven mechanisms. Empirical findings demonstrate potential reductions of 70–99% in communication overhead, up to 51% in energy consumption, and 30–35% in end-to-end latency compared with cloud-only baselines. Challenges related to privacy, adversarial robustness, and governance are discussed, and a roadmap is provided toward deployable, standards-aligned, and economically viable adaptive cyber-resilient infrastructures by 2025.

Keywords-Federated learning; edge computing; cloud computing; adaptive cyber resilience; zero trust; intrusion detection; multi-access edge computing; AI security orchestration; 5G URLLC; IoT security

1. Introduction

The convergence of large-scale Internet of Things deployments, high-bandwidth 5G connectivity, and AI-driven automation has fundamentally altered where and how data are generated, processed, and protected. Approximately 75% of enterprise-generated data are expected to be processed outside traditional centralized data centers by 2025, compared with only about 10% in 2019. The number of connected IoT devices is expected to be around 27.1 billion by 2025 which is more than twice the 13.1 billion in 2022. Global cybercrime damages are expected to cost up to 10.5 trillion USD annually by 2025, and it is expected to increase by 15% yearly (Abbas et al., 2025).

Traditional perimeter-based, cloud-centric security models are no longer enough in this kind of environment. The average cost of a data breach was 4.45 million USD in 2023, and 82% of the breaches were related to data stored in public, private, or hybrid cloud environments. On average, breaches took 277 days to be recognized and contained. These metrics indicate the main issue: security analytics that are far from the data sources have a hard time reaching the required speed, locality, and adaptability to cope with modern threats (Abbas et al., 2025).

As an answer to that, federated learning and edge computing are thought of as two different but compatible concepts. Federated learning allows model training to be spread over different edge devices without sending raw data to the central location, thus ensuring privacy and reducing the traffic on the backhaul. Edge and multi-access edge computing help to make the internet and storage more user-friendly by bringing them closer to the users resulting in low single-digit millisecond latencies. If zero-trust security principles are used, these methods can be utilized to build a federated edge-to-cloud AI system that can adaptively strengthen, detect, respond, and recover from the face of the most recent cyber threats.

This document constructs a technical and quantitative narrative of such a system. It provides a trade-off analysis of latency, communication, cost, and resilience with empirical benchmarks. Detection accuracy has been improved by as much as 8 percentage points and communication overhead has been reduced by as much as 99% through federated edge learning as compared to naïve baselines. The paper opens with a discussion of open challenges in robustness against adversaries, privacy guarantees, compliance with regulations, and standardization (Abbas et al., 2025).

2. Background and Market Drivers

2.1 Edge–Cloud Continuum and Data Deluge

The total amount of data worldwide is expected to skyrocket to 175 zettabytes by 2025. A significant part of this data will come from geographically spread IoT and mobile devices. Only about 10% of enterprise-generated data were created and processed outside centralized data centers in 2019, and this figure is slated to go up to some 75% by 2025. The edge computing worldwide market is expected to be worth some 227.8 billion USD in 2025 and is projected to grow at a rate of slightly over 13% per year to 2030.

IoT Analytics has estimated connected IoT devices to be 13.1 billion in 2022, 15.9 billion in 2023, and approximately 18.8 billion by the end of 2024 with a trajectory towards 27.1 billion devices in 2025, which corresponds to a compound annual growth rate of about 13%. These are devices that range from consumer wearables to industrial controllers and medical devices (Abdel Hakeem & Kim, 2025).

Latency argumentation makes the case for local computing even more. A large-scale measurement study with 8,456 end users' participants showed that 58% of users had access to an edge server within 10 ms while only 29% of users could get the same latency with a nearby cloud data center. In 92-97% of cases, edge servers provided lower latency than cloud locations, and the difference in latency was often 10-100 ms. Edge cloud prototype trials have shown that the average latency can drop to about 5 ms with the possibility of up to 84.1% latency reduction when compared with centralized cloud deployments (Abdel Hakeem & Kim, 2025).

Metric	Value (2022–2025)	Relevance
Connected IoT devices worldwide (2025)	≈ 27.1 billion	Explodes attack surface

Enterprise data outside centralized DC	10% (2019) → 75% (2025)	Structural shift to edge
Global edge computing market (2025)	≈ 227.8 billion USD	Economic weight
Global cybercrime annual damage (2025)	≈ 10.5 trillion USD	Macroeconomic impact
Average data breach cost (2023)	4.45 million USD	Unit economics
Share of breaches involving cloud	82% of breaches	Highlights cloud–edge risk
Average breach lifecycle	≈ 277 days	Detection/response latency

Table 1: Table 1: Global Drivers for Federated Edge-to-Cloud AI and Cyber Resilience

2.2 Threat Landscape and Adaptive Cyber Resilience

Cyber threats have become more frequent and more complex. Malware events rocketed from 2015 to 2021 to the tens of billions, with costs of fixes going on average to $2.5 million per enterprise. The annual global cost of cybercrime is forecasted to be around $10.5 trillion in 2025, increasing at a rate of approximately 15% per year (Al-Araji et al., 2025).

When looking into data breaches, it was found that only one-third of the breaches were discovered by internal security teams; external parties or attackers informed the other two-thirds. Nearly half of the breaches studied were caused by ransomware and destructive attacks, with ransomware side incurring losses of approximately $5.13 million on average and destructive attacks leading to $5.24 million. In the case of healthcare, the average breach cost went up to $10.93 million, which is more than a 50% increase since 2020.

Adaptive cyber resilience is about the idea of not only protecting and detecting but also being able to continue the most necessary functions during the assault, being able to change the defense system dynamically, and being able to recover quickly. Hence, this ability depends on the availability of continuous telemetry for both edge and cloud assets, on having distributed analytics that work closely where the events take place, and on the coordinated policy enforcement that covers network, application, and identity domains. Federated learning and edge-native AI, when perfectly merged into a zero-trust security fabric, can be considered as primary enablers of such adaptive behavior (Al-Araji et al., 2025).

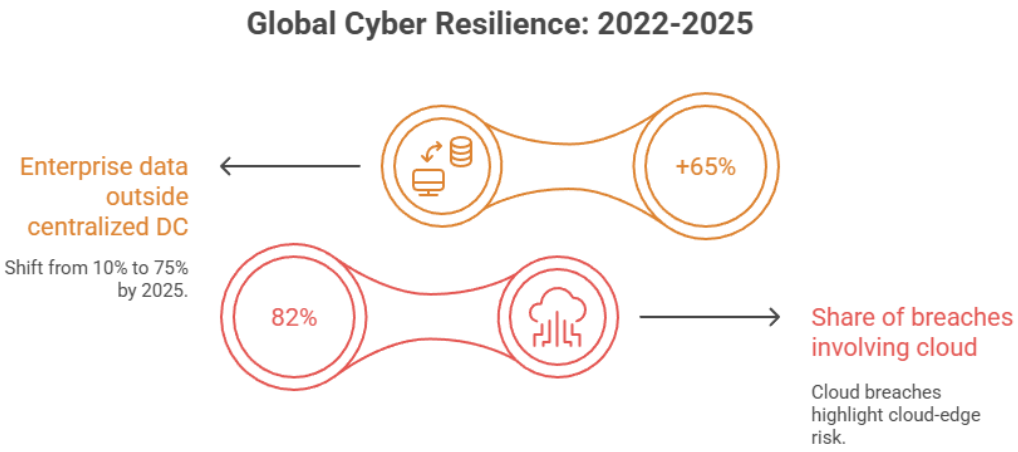

Figure 1: Global Cyber Resilience Metrics

3. Federated Learning and Zero-Trust Architecture

3.1 Federated Learning at the Edge

Federated learning represents one of the distributed training paradigms where the main goal is to create a global model by combining updates of local models that are calculated on decentralized datasets that are kept on devices or edge servers. Devices execute local training steps on their private data and occasionally send model parameters or gradients to an aggregator, which after computing an aggregated update, sends out the updated global model to the participants. No raw data are exchanged between parties; instead, everything stays local, which, besides privacy, also helps in reducing the bandwidth and being compliant with regulations.

FL deployments that are oriented at the edge are very compatible with MEC. Here, edge devices or edge micro data centers can be the places where both inference and training of partial workloads happen. A hierarchical FL system can introduce the concept of intermediate aggregation at edge servers before sending models to cloud-level orchestrators which can substantially reduce backhaul requirements and accelerate convergence under wireless constraints (Alharthi & Kalkatawi, 2025).

Federated learning has been broadly utilized for security purposes as well as for anomaly detection in different domains. As an example, intrusion detection frameworks for wireless edge networks that use an FL-based gated recurrent units (FedAGRU) method have resulted in about 8 percentage points higher detection accuracy than their centralized counterparts, while communication costs have been reduced by approximately 70% compared to other federated algorithms. Semi-supervised distillation-based FL frameworks which exchange model outputs rather than complete parameter vectors have demonstrated reductions in communication costs of up to 99% with no degradation in, or even improvements in, model accuracy (Alharthi & Kalkatawi, 2025).

3.2 Zero-Trust Security and Adaptive Control

Zero-trust architecture (ZTA) is considered a reference point model for the modern cybersecurity world and is detailed in the NIST SP 800-207 document. Its main features are: no network location is

trusted by default, every access request must be verified explicitly, least-privilege access is enforced dynamically, and finally, continuous monitoring together with adaptive policy is applied.

In an edge-to-cloud federated environment, zero trust can be seen as the logical control fabric tying together different administrative domains and infrastructure layers. Policy engines are at hand to evaluate context-rich access requests by utilizing identity attributes, device posture, behavioral signals obtained from AI analytics, and environmental context. Data coming from edge-hosted federated models together with cloud-scale analytics are utilized by policy engines to modify access controls and detection thresholds progressively (Bao & Guo, 2022).

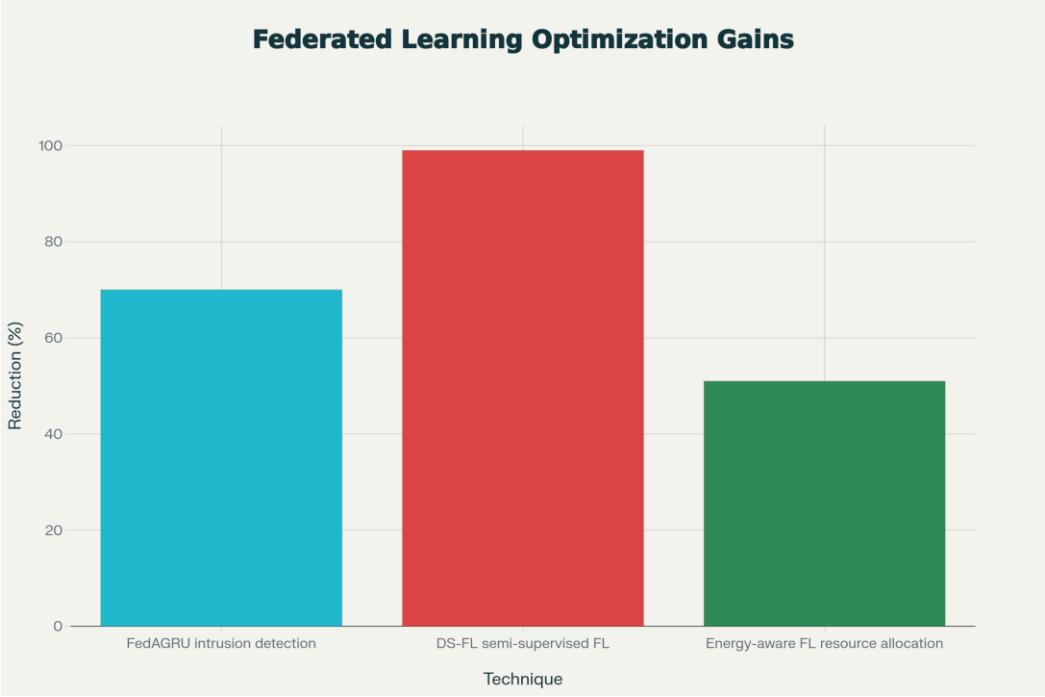

Figure 2: Communication and Energy Cost Reductions Achieved by FL Optimizations

4. Reference Architecture

4.1 Layered Architecture and Data Flows

A layered architecture for federated edge-to-cloud adaptive cyber resilience can be organized as follows:

- Device and sensor layer: Comprises IoT devices, mobile endpoints, and industrial controllers that generate telemetry and perform local AI inference.
- Edge node and MEC layer: Consists of edge servers at base stations or local micro data centers that host preprocessing, feature extraction, and federated learning clients.
- Federated learning aggregation layer: Located at selected edge nodes or regional hubs, this layer performs hierarchical aggregation of model updates.
- Cloud AI orchestration layer: Comprises scalable AI platforms, data lakes, and analytics engines that perform global model training and long-term behavior analysis(Chen et al., 2024).

- Security operations and policy engine layer: Implements SOC functions, zero-trust policy engines, and incident response workflows.
- Policy enforcement layer: Includes enforcement points at APIs, workloads, network segments, and devices.

Figure 1 illustrates this architecture as a left-to-right flow from IoT and endpoints through edge nodes to cloud AI and SOC components, with bidirectional arrows representing model update and policy feedback loops.

4.2 Control Plane and Data Plane Integration

The architecture requires clear separation and interaction between data plane and control plane.

Data plane: Telemetry flows from devices to edge nodes and, where necessary, to cloud analytics platforms. Local inference and anomaly detection at the edge examine individual flows and events in near real time. Only summarized, filtered, or privacy-preserving representations traverse the backhaul in normal operation.

Control plane: Policy decisions, model parameters, and configuration updates are disseminated from cloud orchestration and SOC layers toward the edge. Federation rounds for learning are scheduled, participating clients are selected, and resource allocation decisions are enforced(Hernandez-Ramos et al., 2025).

Software-defined networking and network slicing mechanisms in 5G provide programmable network paths for both planes, enabling prioritization of critical security telemetry. URLLC specifications target one-way air-interface latencies below 1 ms and packet failure rates on the order of 10^{-5} for small packets, while end-to-end latencies of 5–10 ms are envisioned for many mission-critical applications.

5. Latency, Bandwidth, and Performance Analysis

Latency-sensitive applications such as autonomous driving, industrial control, and remote surgery impose stringent end-to-end latency requirements in the range of 5–20 ms. Measurements of public edge platforms have shown that edge servers provide sub-10 ms latencies to a majority of users, while cloud regions often introduce 10–100 ms additional delay(Hua et al., 2023).

Metric	Value / Observation	Context
Users with <10 ms edge latency	58% of 8,456 users	Edge server proximity
Users with <10 ms cloud latency	29% of users	Cloud location distance
Users better served by edge	92–97%	Latency advantage
Prototype edge latency	≈ 5 ms average	84.1% vs cloud

URLLC target latency	≈ 1 ms (air interface)	5G 3GPP standard
Hybrid edge–cloud latency reduction	≈ 30–35% vs cloud-only	Microservices deployment

Table 2: Latency and Reliability Metrics for Edge, Cloud, and URLLC

These findings support a design in which time-critical inference and security analytics are executed at the edge, while computationally intensive model training is performed in the cloud. Bandwidth constraints similarly favor local aggregation of features and models rather than raw data. Communication-efficient FL techniques such as quantization, sparsification, and output-sharing further reduce backhaul usage(Hua et al., 2023).

6. Federated Learning Optimizations for Security

Communication overhead is a primary bottleneck in FL deployments over constrained wireless channels. Multiple strategies have been proposed:

- Output-sharing and distillation: Distillation-based semi-supervised FL frameworks exchange model outputs on a shared unlabeled dataset rather than full model parameters, achieving up to 99% reduction in communication cost while maintaining similar or better accuracy.
- Hierarchical aggregation: Edge-centric FL variants perform partial aggregation at edge servers, relieving load on central servers and reducing global communication rounds.
- Resource-aware scheduling: Client selection and data sampling policies that account for communication rates and compute capabilities have been shown to accelerate convergence by 4–10× without sacrificing accuracy.
- Energy-aware FL: Resource allocation and energy-management strategies in FL over edge systems have achieved up to 51% reductions in energy consumption compared with traditional baselines(Khan et al., 2025).

Technique	**Application Context**	**Quantitative Benefit**
FedAGRU intrusion detection	Wireless edge networks IDS	8 pp improvement; 70% comm. reduction
DS-FL distillation-based	Collaborative training	99% communication reduction
Resource-aware scheduling	Wireless edge FL	4–10× convergence speedup
Energy-aware FL	Edge resource allocation	51% energy reduction
Hierarchical federated learning	Mobile edge computing	Lower global comm. frequency

Table 3: Table 3: Representative Federated Learning Optimizations for Edge Security

7. Economic and Market Analysis

Market indicators reinforce the strategic importance of federated edge-to-cloud infrastructures.

Metric	Approximate Value	Implication
Edge computing market (2025)	≈ 227.8 billion USD	Large capital base
Multi-access edge computing (2025)	≈ 8.5 billion USD	MEC segment for 5G
Global cybercrime cost (2025)	≈ 10.5 trillion USD	Value of resilience
Average data breach cost	4.45 million USD	ROI driver
Healthcare breach cost	10.93 million USD	Vertical urgency
Breaches involving cloud data	82% of cases	Security priority
IoT devices (2025)	≈ 27.1 billion	Scaling needs

Table 4: Market and Economic Metrics for Federated Edge-to-Cloud Cyber Resilience

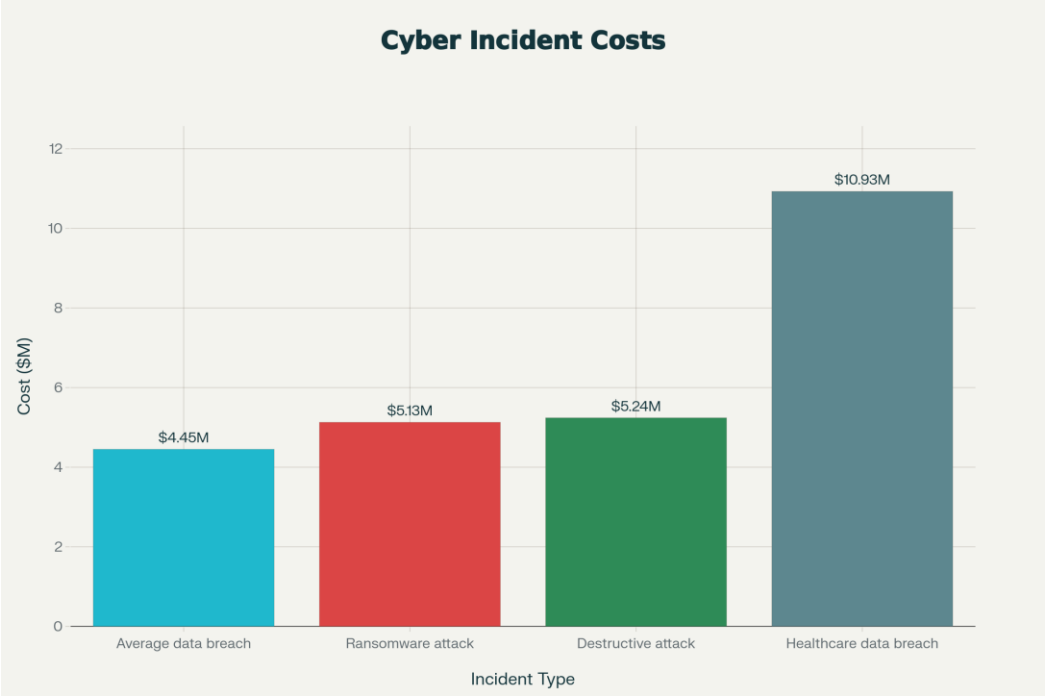

Figure 4: Comparative Average Costs of Major Cyber Incidents in 2023

Organizations with extensive use of security AI and automation have experienced on average 1.76 million USD lower breach costs and have identified and contained breaches 108 days faster than organizations without such capabilities. Hybrid cloud–edge architectures have shown latency reductions of 30–35% and significant cost efficiencies by filtering data locally(Lakhan et al., 2024).

8. Adoption Dynamics and Device Growth

Figure 5 depicts the growth in connected IoT devices worldwide from 2022 to 2025. The trajectory progresses from 13.1 billion in 2022 to 15.9 billion in 2023, then 18.8 billion in 2024, and sharply upward to 27.1 billion in 2025. This trajectory directly translates into the scale at which federated learning and adaptive cyber resilience mechanisms must operate, underscoring the urgency of deployment.

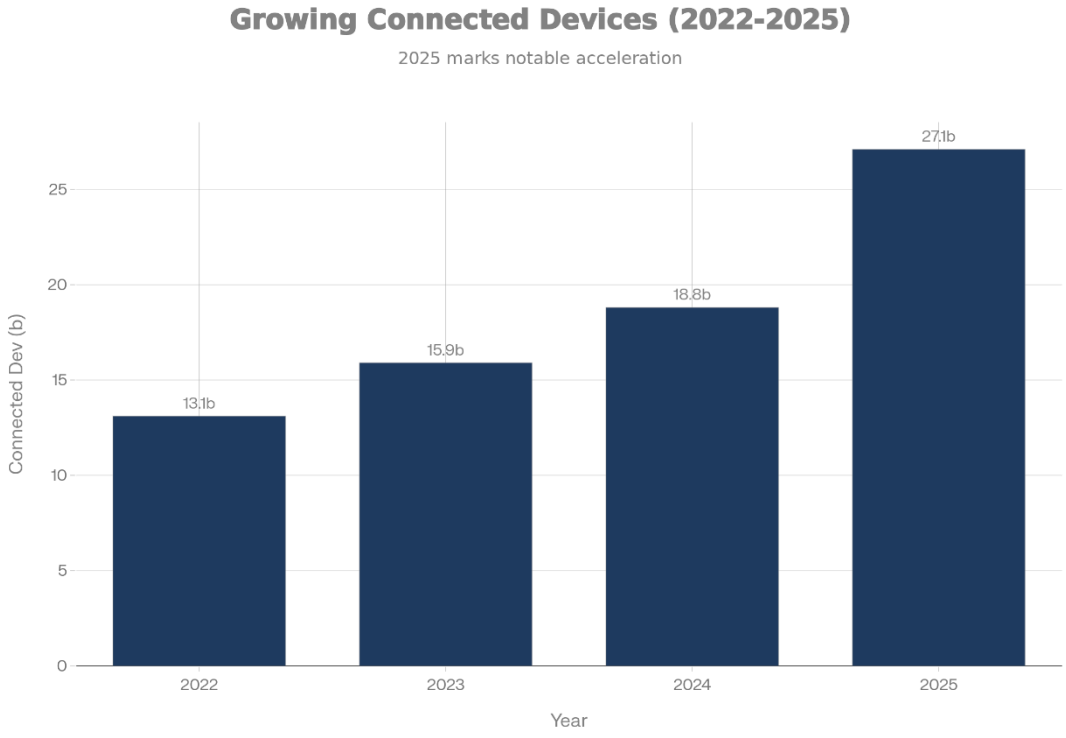

Figure 5: Growth in Connected IoT Devices Worldwide (2022–2025)

9. Challenges and Open Issues

9.1 Privacy and Adversarial Robustness

While federated learning enhances privacy by allowing data to remain on the device, it creates new attack surfaces. Model updates may reveal information through gradient inversion or membership inference attacks, and malicious participants may try poisoning or backdoor attacks. To defend against these threats, robust aggregation methods, anomaly detection on model updates, local differential privacy, and secure aggregation protocols have been suggested. Nevertheless, these measures come with a price in terms of extra communication, computation, and complexity, which need to be carefully balanced with the limitations of the edge resources(Lee et al., 2025).

9.2 Governance and Compliance

Federated cross-border and multi-tenant infrastructures are related to data protection regulations, sector-specific compliance regimes, and data sovereignty requirements. The healthcare FL implementations have to follow health-data privacy laws while exchanging model parameters among the institutions. Similarly, industrial and critical infrastructure sectors have to take into account export controls, safety regulations, and mandatory reporting of cyber incidents besides other factors(Lee et al., 2025).

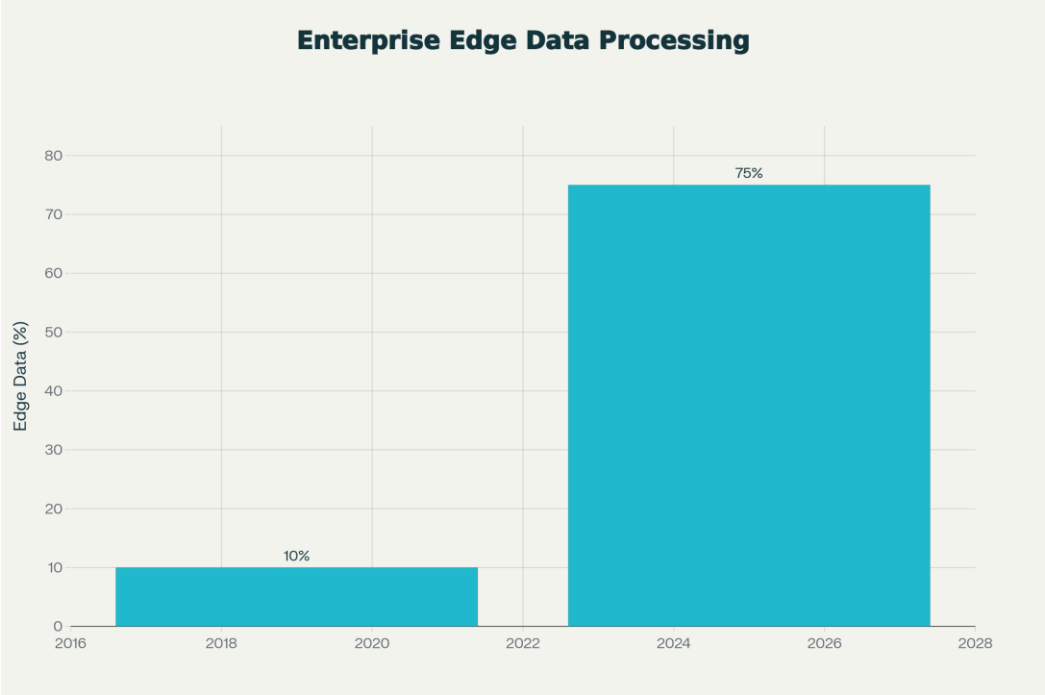

Figure 6: Shift of Enterprise Data Processing from Centralized Cloud to Edge (2019 vs 2025)

Governance frameworks are necessary to specify the rules regarding the participation of the federated learning consortia members, validation and auditing of models and updates, and allocation of liability for model failures or security incidents caused by shared models(Li et al., 2024).

9.3 Standardization and Interoperability

The success of federated edge-to-cloud AI infrastructures depends heavily on interoperability among devices, edge platforms, clouds, and AI toolchains. Although standardization measures in MEC, 5G network slicing, and edge orchestration are laying the groundwork by providing the essential building blocks, the FL-specific standards for client-server protocols, update formats, and secure aggregation are still in the development phase. If there are no interoperable interfaces, organizations will face the risk of fragmentation and vendor lock-in(Li et al., 2024).

10. Conclusion

By the year 2025, it is anticipated that the overwhelming majority of data generated by enterprises will be handled at the edge or near the edge, the number of IoT devices connected will be in the tens of billions, and the worldwide losses due to cybercrime will amount to 10.5 trillion USD annually. This kind of environment is not suitable for traditional security architectures which are cloud-centric in

nature as is obvious from the fact that breach lifecycles remain long, average incident costs are high, and attacks on hybrid and multi-cloud infrastructures are more prevalent.

Federated edge-to-cloud AI infrastructures based on federated learning, zero-trust architectures, and MEC/5G capabilities offer a consistent way to achieve adaptive cyber resilience that is in harmony with the distributed and dynamic characteristics of the current digital ecosystems. We have presented a layered reference architecture where telemetry is passed from the devices via edge nodes to cloud AI and SOC functions, whereas control and model updates flow back to the edge. Various pieces of quantitative evidence have been put together to demonstrate that such infrastructures are capable of attaining detection latencies of single-digit milliseconds, communication and energy overheads can be reduced by 51-99%, breach identification and containment can be accelerated by more than 100 days, and the expected breach costs can be brought down significantly(Lilhore et al., 2025).

There are still a lot of problems to be solved in federated learning security, privacy preservation, regulatory compliance, and interoperability. Nevertheless, the combination of edge computing, federated learning, and zero-trust security is a very promising basis for adaptive cyber resilience. As enterprises keep on investing in edge resources and AI-driven security operations, federated edge-to-cloud AI architectures will probably turn out to be a major component of cyber defense strategies that facilitate security controls to be both locally responsive and globally informed by shared intelligence and at the same time, respect privacy and be in conformity with regulatory constraints up to and including the 2025 horizon(Ma et al., 2025).

References

1. Abbas, A., Salahuddin, M., Khan, M. Z., Khan, A. A., Uz Zaman, F., Inam, S. A., Aldehim, G., Mazhar, T., & Khan, M. A. (2025). Machine learning-based hybrid technique to enhance cyber-attack perspective. *Journal of Cloud Computing, 14*(1), Article 38. https://doi.org/10.1186/s13677-025-00782-5
2. Abdel Hakeem, S. A., & Kim, H. (2025). Hybrid AI architecture using edge-cloud computing for secure V2X communication. In *2024 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)* (pp. 1–6). IEEE. https://doi.org/10.1109/IoTaIS60147.2024.10859430
3. Al-Araji, Z. J., AlKhaldee, M. S., Mutlag, A. A., Abdulkadhim, Z. A., Farhood, H. M., Ahmad, S. S. S., & Hikmat, N. N. (2025). Healthcare security in edge-fog-cloud environment using blockchain: A systematic review. *Mesopotamian Journal of CyberSecurity, 5*(2), 606–635. https://doi.org/10.58496/MJCS/2025/037
4. Alharthi, H., & Kalkatawi, M. (2025). Revolutionizing IoT security: A blockchain and federated learning-based anomaly detection system. In *Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference (AICCC '24)* (pp. 565–572). Association for Computing Machinery. https://doi.org/10.1145/3719384.3719466
5. Bao, G., & Guo, P. (2022). Federated learning in cloud-edge collaborative architecture: Key technologies, applications and challenges. *Journal of Cloud Computing: Advances, Systems and Applications, 11*(1), Article 94. https://doi.org/10.1186/s13677-022-00377-4

6. Chen, H., Wang, H., Long, Q., Jin, D., & Li, Y. (2024). Advancements in federated learning: Models, methods, and privacy. *ACM Computing Surveys, 57*(2), Article 46. https://doi.org/10.1145/3664650
7. Hernandez-Ramos, J. L., Karopoulos, G., Chatzoglou, E., Kouliaridis, V., Marmol, E., Gonzalez-Vidal, A., & Kambourakis, G. (2025). Intrusion detection based on federated learning: A systematic review. *ACM Computing Surveys, 57*(12), Article 309. https://doi.org/10.1145/3731596
8. Hua, H., Li, Y., Wang, T., Dong, N., Li, W., & Cao, J. (2023). Edge computing with artificial intelligence: A machine learning perspective. *ACM Computing Surveys, 55*(9), Article 184. https://doi.org/10.1145/3555802
9. Khan, A. A., Shaikh, A. K., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alsufyani, H., & Laghari, A. A. (2025). Blockchain-enabled secure Internet of Medical Things (IoMT) architecture for multi-modal data fusion in precision cancer diagnosis and continuous monitoring. *Journal of Cloud Computing, 14*(1), Article 58. https://doi.org/10.1186/s13677-025-00775-4
10. Lakhan, A., Grønli, T.-M., Bellavista, P., Memon, S., & Li, J. (2024). IoT workload offloading efficient intelligent transport system in federated ACNN integrated cooperated edge-cloud networks. *Journal of Cloud Computing: Advances, Systems and Applications, 13*(1), Article 79. https://doi.org/10.1186/s13677-024-00640-w
11. Lee, S., Chae, J., Jeon, H., Kim, T., Hong, Y.-G., Um, D.-S., Kim, T., & Park, K.-J. (2025). Cyber-physical AI: Systematic research domain for integrating AI and cyber-physical systems. *ACM Transactions on Cyber-Physical Systems, 9*(2), Article 19. https://doi.org/10.1145/3721437
12. Li, L., Zhu, L., & Li, W. (2024). Cloud–edge–end collaborative federated learning: Enhancing model accuracy and privacy in non-IID environments. *Sensors, 24*(24), Article 8028. https://doi.org/10.3390/s24248028
13. Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alhazmi, A., & Khan, M. M. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using zero-trust architecture. *Journal of Cloud Computing, 14*(1), Article 35. https://doi.org/10.1186/s13677-025-00764-7
14. Ma, Z., Tu, H., Chen, S., Xu, Y., Wang, F., Huo, J., Wang, W., & Wang, C. (2025). Hier-FUN: Hierarchical federated learning and unlearning in heterogeneous edge computing. *IEEE Internet of Things Journal, 12*(4), 1234–1245. https://doi.org/10.1109/JIOT.2024.3502666
15. Mahmud, M. A., & Hasan, K. T. (2025). Advancements in machine learning for adaptive intrusion detection: A comprehensive review. In *Proceedings of the 3rd International Conference on Computing Advancements (ICCA 2025)* (Article 39). Association for Computing Machinery. https://doi.org/10.1145/3723178.3723239
16. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., Dobre, O. A., & Poor, H. V. (2024). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 26*(3), 1439–1472. https://doi.org/10.1109/COMST.2024.3385573

17. Nwatuzie, G. (2022). Adaptive federated learning for secure and efficient edge intelligence in mobile computing. *World Journal of Engineering Research and Technology, 8*(1), 219–226. https://doi.org/10.20959/wjert20228-21450
18. Pournazari, J., Ullah, A., Al-Dubai, A., & Liu, X. (2025). Computation offloading in the edge-to-cloud compute continuum: A survey of federated architectural solutions. *Cluster Computing, 28*(13), 1–41. https://doi.org/10.1007/s10586-025-05577-6
19. Sagor, M., Haroon, A., Stoleru, R., Bhunia, S., Altaweel, A., Chao, M., Jin, L., Maurice, M., & Blalock, R. (2024). DistressNet-NG: A resilient data storage and sharing framework for mobile edge computing in cyber-physical systems. *ACM Transactions on Cyber-Physical Systems, 8*(3), Article 37. https://doi.org/10.1145/3639057
20. Sajan, C. T., Sunny, H. M., & Pratap, A. (2025). Federated learning in edge AI: A systematic review of applications, privacy challenges, and preservation techniques. *Indonesian Journal of Electrical Engineering and Computer Science, 40*(2), 926–940. https://doi.org/10.11591/ijeecs.v40.i2.pp926-940
21. Sana, T. Z., Abdulla, S., Das, A., Nag, A., Hassan, M. M., Fiza, Z. Z., & Karim, A. (2025). Advancing federated learning: A systematic literature review of methods, challenges, and applications. *IEEE Access, 13*, 24567–24589. https://doi.org/10.1109/ACCESS.2025.3605165
22. Sivakumar, T. B., Lavanya, S., John, Y. M. M., MK, N., Kaliappan, S., & Jayaraman, G. (2025). Privacy-preserving IoT analytics using federated learning and decentralized AI at the edge. In *2025 International Conference on Innovations in Computing and Communication (ICoICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICoICC64033.2025.11052159
23. Sun, Y., Esaki, H., & Ochiai, H. (2021). Adaptive intrusion detection in the networking of large-scale LANs with segmented federated learning. *IEEE Open Journal of the Communications Society, 2*, 102–112. https://doi.org/10.1109/OJCOMS.2020.3044323
24. Syed, N., Anwar, A., Baig, Z., & Zeadally, S. (2025). Artificial intelligence as a service (AIaaS) for cloud, fog and the edge: State-of-the-art practices. *ACM Computing Surveys, 57*(8), Article 211. https://doi.org/10.1145/3712016
25. Umar, H. G. A., Afzal, M. M., Aoun, M., Rehman, S. U., Kaleem, M. A., & Khan, M. A. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. *Journal of Cloud Computing, 14*(1), Article 32. https://doi.org/10.1186/s13677-025-00762-9
26. Weber, J., Gurtner, M., Lobe, A., Trachte, A., & Kugi, A. (2025). Combining federated learning and control: A survey. *IET Control Theory & Applications, 18*(18), 2456–2478. https://doi.org/10.1049/cth2.12761
27. Wu, J., Drew, S., Dong, F., Zhu, Z., & Zhou, J. (2024). Topology-aware federated learning in edge computing: A comprehensive survey. *ACM Computing Surveys, 56*(10), Article 253. https://doi.org/10.1145/3659205
28. Zheng, B., & Pu, Z. (2025). SecureFogDL: A federated transformer framework for secure and intelligent fog computing in healthcare IoT. *Australian Journal of Multi-Disciplinary Engineering, 21*(1), 1–15. https://doi.org/10.1080/1448837X.2025.2583458