

Journal of Computer Science and Technology, Vol 2 (2) 2025: 90-112

TechComp Innovations

https://mabadiiqtishada.org/index.php/TechCompInnovations

ISSN: 3062-8903; e-ISSN: 3062-889X

Federated Intelligence Architectures for Secure, Data-Driven Innovation Across AI, IoT, and Cloud Ecosystems

Ravi Kumar Saidala[1*], Umna Iftikhar[2], Tofig Hasanov[3], Vüqar Ahmad Mammadli[4]

[1] *Department of CSE - Data Science. CMR University. India*

[2] *Faculty of Engineering Science and Technology. IQRA University. Pakistan*

[3] *Dagestan State Agrarian University named after M.M. Dzhambulatov. Russia*

[4] *Mingachevir State University. Azerbaijan*

ARTICLE INFO

Received Dec 2, 2025
Accepted Dec 22, 2025
Published Dec 23, 2025

Keywords:
Federated Intelligence; IoT Ecosystems; Blockchain-enabled Security; Zero-Trust Architecture; Edge AI

ABSTRACT

This study examines the emerging paradigm of federated intelligence architectures as a secure, privacy-preserving, and scalable foundation for data-driven innovation across AI, IoT, and cloud ecosystems. With billions of interconnected devices generating massive heterogeneous data, traditional centralized machine-learning models face critical limitations, including privacy risks, regulatory constraints, latency, and single points of failure. Through a qualitative content-analysis approach, this paper synthesizes contemporary research on federated learning, blockchain integration, zero-trust governance, and edge intelligence to formulate a comprehensive understanding of distributed AI infrastructures. The findings highlight that federated learning enables collaborative model training without exposing raw data, significantly enhancing privacy, security, and compliance. Moreover, combining blockchain with federated learning strengthens auditability, model integrity, and trust, while zero-trust principles provide continuous verification and adaptive security enforcement across devices. Edge-AI integration further reduces latency and bandwidth consumption, enabling real-time analytics in resource-constrained IoT environments. Collectively, these elements contribute to the formation of cognitive ecosystems capable of autonomous, interoperable, and context-aware operations. The study underscores the transformative potential of federated intelligence while identifying critical gaps that inform future research trajectories

How to cite: Saidala, R. K., Iftikhar, U., Hasanov, T., & Mammadli, V. A. (2025). Federated Intelligence Architectures for Secure, Data-Driven Innovation Across AI, IoT, and Cloud Ecosystems. *TechComp Innovations: Journal of Computer Science and Technology*, 2(2), 90–112. https://doi.org/10.70063/techcompinnovations.v2i2.124

This is an open-access article distributed under the Creative Commons 4.0 Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. ©2023 by author.

* *Corresponding author: ravikumar.s@cmr.edu.in*

INTRODUCTION

The burgeoning landscape of artificial intelligence, coupled with the pervasive integration of the Internet of Things and expansive cloud computing infrastructures, presents unprecedented opportunities for data-driven innovation (Chen et al., 2024). However, this rapid proliferation of intelligent devices—projected to reach 32.1 billion IoT connections by 2030—generates immense volumes of data, posing significant challenges for privacy, security, and efficient processing (Wu et al., 2025). Traditional cloud-centric AI architectures often exacerbate these issues through centralized data handling, which introduces single points of failure, latency, and heightened security risks (Ahmad et al., 2024; Thomas & Myakala, 2025).

Federated intelligence architectures offer a compelling alternative, rooted in federated learning, by enabling collaborative model training across distributed data sources without centralizing sensitive information. This decentralized approach mitigates privacy breaches, reduces latency, minimizes network congestion, and enhances resilience against cyber threats while preserving data sovereignty and complying with stringent global privacy regulations such as GDPR (Feng et al., 2024; Ogunbajo et al., 2025; Rahman, 2025; Robai, 2024; Schwermer et al., 2024b, 2024a; Shirvani & Ghasemshirazi, 2024; Zhang et al., 2021). By conducting computations locally on edge devices—like IoT nodes—and transmitting only model updates to a central server, FL addresses critical concerns in expanding IoT deployments, including data privacy, security, and computational efficiency (Aggarwal et al., 2024; Beltrán et al., 2023; Otoum et al., 2025; Rane et al., 2024).

The exponential growth of connected devices and distributed computing has transformed digital infrastructures into interconnected AI-IoT-cloud ecosystems reliant on real-time data processing. Yet, unresolved challenges in privacy, cybersecurity, interoperability, and data governance render traditional centralized models inadequate due to scalability limits and regulatory restrictions (Rahman, 2025). This paper explores the technical underpinnings and practical implications of federated intelligence architectures from a qualitative standpoint, synthesizing theoretical constructs and recent scholarly contributions. Despite its promise, this nascent domain requires comprehensive grounding to support secure, data-driven innovation across interconnected ecosystems (Monteiro et al., 2024).

RESEARCH METHOD

This research adopts a qualitative methodology employing library research and content analysis as its core approach. Library research was conducted by systematically collecting scholarly sources, including journal articles, monographs, conference proceedings, and policy documents addressing federated learning, distributed architectures, IoT intelligence, cloud-native designs, and cybersecurity frameworks. This comprehensive review aimed to identify foundational theories, emerging trends, and critical challenges within these interconnected domains (Ahmad et al., 2024; Barros et al., 2024). The collected literature was then subjected to content analysis, focusing on identifying recurring themes, conceptual models, and architectural patterns related to secure, data-driven innovation across AI, IoT, and cloud ecosystems, with particular attention to how federated intelligence addresses privacy, security, and scalability issues (Rahman, 2025).

These sources were examined through content analysis, focusing on conceptual patterns, recurring theoretical models, and emerging architectural proposals. Coding

techniques were used to extract knowledge elements related to federated intelligence, security concerns, data governance strategies, and interoperability challenges. The synthesized findings were then categorized into five dominant thematic domains that reflect current trends and strategic trajectories in the integration of AI, IoT, and cloud systems. This rigorous qualitative approach allowed for a deep understanding of the complex interdependencies and novel solutions offered by federated intelligence in fostering secure, data-driven innovation (Schwermer et al., 2024). Specifically, the analysis delves into advanced cryptographic techniques, secure multi-party computation mechanisms, and differential privacy approaches underpinning these federated AI models (Ogunbajo et al., 2025).

This systematic review aims to delineate the current state of federated learning applications, particularly concerning security, privacy, and compliance issues within cloud computing (Albshaier et al., 2025). It also seeks to provide a conceptual framework for integrating federated intelligence with robust security protocols to facilitate trusted, data-driven innovation across distributed ecosystems (Uddoh et al., 2021). Innovative approaches such as blockchain for audibility, differential privacy for re-identification prevention, and clustering techniques for personalization are among the solutions analyzed (Uddin et al., 2024). The qualitative approach further scrutinized how AI-driven access control mechanisms and homomorphic encryption contribute to enhanced privacy preservation in IoT-based cloud environments (Dhinakaran et al., 2024). The meticulous selection process adhered to PRISMA guidelines, ensuring that only peer-reviewed literature from major scientific databases published between 2016 and 2024 was considered, thereby reflecting the most current advancements and challenges in the field (Olagunju, 2025).

RESULT AND DISCUSSION

Federated Learning as the Core of Distributed Intelligence

Federated learning (FL) provides the technical foundation enabling multiple nodes—such as IoT sensors, edge devices, and cloud servers—to collaboratively train machine learning models without sharing raw data. By transmitting only gradients or model updates, FL preserves confidentiality while retaining the benefits of collective intelligence. This distributed training paradigm reduces exposure to data breaches, aligns with data localization laws, and supports computing at the network's edge. This capability is particularly vital in environments where data privacy and governance are paramount, ensuring that sensitive information remains within its originating domain (Ahmad et al., 2024; Vyhmeister & Castañé, 2024). Furthermore, the application of robust encryption methods such as fully homomorphic encryption and SHA-3 is critical for safeguarding the integrity and confidentiality of these model updates during transit and at rest within cloud computing environments (Pothireddy et al., 2024). Moreover, secure aggregation protocols are essential to prevent inference attacks on shared model parameters, further bolstering the privacy guarantees of federated learning systems (Ahmad et al., 2024).

This decentralized approach minimizes the attack surface traditionally associated with centralized data repositories, distributing the risk across numerous independent entities rather than concentrating it in a single point of failure (Rahmati, 2025). This architectural shift significantly enhances the overall security posture against various cyber threats by obviating the need for a central repository of sensitive data (Pothireddy et al., 2024). Consequently, federated learning facilitates data-driven innovation even in stringent regulatory landscapes by enabling collaborative intelligence without direct data exchange, thereby fostering broader

participation across diverse organizations (Narkedimilli et al., 2024). This distributed paradigm not only enhances data privacy but also reduces communication overheads by processing data closer to its source, leading to more efficient and scalable AI deployments (Erdal et al., 2024). The collaborative nature of federated learning allows algorithms to learn from experiences accumulated across various devices without aggregating data from multiple sources, addressing critical privacy and regulatory concerns (Monteiro et al., 2024; Puppala et al., 2024; Rahman, 2025).

Specifically, FL enables the training of models on distributed datasets without direct access to sensitive information, promoting privacy-preserving machine learning across diverse ecosystems (Campos et al., 2024; Zhao et al., 2025). This approach addresses the computational power and training duration challenges often associated with traditional centralized machine learning, while notably enhancing security and privacy (Aggarwal et al., 2024). The inherent privacy-preserving nature of FL arises from clients training sub-models locally and sending only encrypted updates to a central server for aggregation into a global model, significantly mitigating the risks of data breaches and information theft (Shen et al., 2020). This method inherently reduces privacy risks as clients maintain their data locally, and only model updates, not raw data, are transmitted to the central server (Huang et al., 2024). This design aligns with stringent data protection regulations such as GDPR, as it ensures user control over personal data and minimizes the exposure of sensitive information (Zhao et al., 2025; Zhu et al., 2024).

The scalability of FL is further boosted through its ability to leverage cloud computing and distributed systems, optimizing resource utilization by incorporating contributions from multiple clients (Deshmukh et al., 2025). This distributed training paradigm is particularly advantageous for applications requiring real-time processing and low latency, as it minimizes the need for extensive data transfers to a centralized server (Himeur et al., 2023). Moreover, federated learning inherently supports compliance with regulatory frameworks such as GDPR and HIPAA by ensuring that sensitive data remains localized, thus avoiding cross-border data transfer issues and enhancing data governance (Barbosa et al., 2025; Rane et al., 2024). This decentralization inherently minimizes bandwidth and latency concerns, making it exceptionally well-suited for real-time applications such as augmented reality and metaverse platforms in healthcare (Rauniyar et al., 2023).

The conventional reliance on centralized machine learning approaches, which aggregate raw data in cloud infrastructures, poses significant scalability and compliance limitations, particularly in distributed environments with a multitude of interconnected devices generating varied data (Mahmood et al., 2025). In contrast, federated learning emerges as a potent alternative, facilitating collaborative model training across a diverse ecosystem of devices and institutions without requiring raw data aggregation, thereby mitigating privacy concerns and enhancing data security (Abbas et al., 2024; Madathil et al., 2025). This decentralized paradigm, first introduced by Google in 2017, facilitates improved predictive text models on Android devices by keeping sensitive user data on local devices while enabling collaborative model training (Monteiro et al., 2024). This innovation marked a pivotal shift towards privacy-preserving AI, allowing for model improvements without compromising user data (Sen et al., 2024; Sumanth et al., 2023).

IoT as a Real-Time Data Acquisition Layer

Within federated architectures, IoT devices serve as data sources and autonomous inference engines capable of executing localized computations. The shift toward intelligent IoT nodes—

enhanced with embedded AI models—enables real-time analytics at the periphery of the network. This reduces dependency on centralized servers, lowers latency, and supports mission-critical applications such as smart factories, precision agriculture, and autonomous logistics. This local processing capability is crucial for scenarios demanding immediate responsiveness and for environments where continuous connectivity to a central cloud is unreliable or bandwidth-limited (Rane et al., 2024; Sammangi et al., 2025). Moreover, Medical Internet of Things devices, such as wearable heart monitors and smart insulin pumps, leverage this edge processing to provide real-time diagnostics and personalized treatment, even with limited resources and sensitive data (Garg, 2025). This distributed intelligence approach, wherein data evaluation occurs locally on edge devices, is a cornerstone of federated learning, ensuring data privacy for IoT devices, especially in sensitive domains like healthcare (Rauniyar et al., 2023).

This setup allows for the training of robust machine learning models without the need to transfer sensitive patient data to a centralized server, addressing major privacy concerns (Lin & Wen, 2024; Zhang et al., 2021). This ensures that confidential medical records remain secure on local devices, thereby complying with stringent regulations like HIPAA (Shirvani & Ghasemshirazi, 2024; Yang et al., 2025). This decentralized processing also significantly mitigates the communication burden on networks, as only model updates, rather than voluminous raw data, are transmitted for global model aggregation (Albelaihi, 2025). This approach revolutionizes healthcare by enabling collaborative machine learning across institutions while preserving patient privacy and meeting regulatory standards (Abbas et al., 2024).

Furthermore, federated learning improves operational efficiency and service personalization in sectors like healthcare, manufacturing, and urban management by enabling data-driven decisions while safeguarding sensitive information (Marengo, 2024). The integration of federated learning with edge intelligence further optimizes this paradigm, allowing for more efficient local data processing and real-time inference on resource-constrained IoT devices (Mughal et al., 2024; Nori et al., 2021). This combined architecture enhances privacy, reduces latency, and optimizes bandwidth usage by processing data closer to its source, which is particularly beneficial in scenarios with limited connectivity or high data volumes (Boruga et al., 2024). This synergy between federated learning and edge AI is particularly impactful in healthcare, enabling real-time monitoring and personalized recommendations directly on wearable devices without compromising patient data (Rane et al., 2024).

This approach not only facilitates early detection of health irregularities but also permits swift responses to potential emergencies, all while upholding patient data privacy by minimizing the necessity for extensive data transmission for analysis (Li et al., 2023). This local processing capability is further enhanced by edge analytics, which enables real-time data preprocessing, anomaly detection, and feature extraction directly at the data source, significantly reducing latency and computational overhead associated with traditional cloud-based federated learning (Munusamy & Jothi, 2025). This minimization of transmitted data, coupled with reduced bandwidth usage, accelerates decision-making processes and enhances overall system responsiveness and energy efficiency (Munusamy & Jothi, 2025). This convergence of Edge-AI and federated learning is particularly transformative for the Industrial Internet of Things, where decentralized model training reduces energy consumption, enhances privacy, and mitigates bandwidth constraints (Kumar et al., 2025).

However, despite these advantages, conventional federated learning frameworks still encounter considerable challenges, including high computational demands on edge devices, significant communication latency from frequent model updates, and vulnerabilities to poisoning attacks, which collectively impede their scalability and trustworthiness in large-scale deployments (Munusamy & Jothi, 2025a, 2025b). To address these critical limitations, novel architectural advancements are imperative, especially considering the constraints of transmitting large datasets for training and the need to keep sensitive information localized (Sánchez et al., 2025). One such advancement involves integrating blockchain technology to ensure secure aggregation mechanisms, tamper-proof model updates, and decentralized accountability (Thomas & Myakala, 2025). This integration establishes a transparent and immutable ledger for all transactions, enhancing trust and auditability in federated AI ecosystems (Cheikh et al., 2025). Moreover, blockchain's inherent characteristics of transparency, immutability, and decentralization provide a robust foundation for secure data sharing and model versioning within federated environments (Li et al., 2025).

This distributed ledger technology ensures that each model update and data transaction is verifiable and resistant to tampering, addressing critical security concerns in sensitive applications such as healthcare and finance (Jasim & Hadi, 2025; Li et al., 2025). Beyond mere security, blockchain also facilitates robust data provenance and integrity verification, which are essential for maintaining the trustworthiness of shared AI models across diverse stakeholders (Jasim & Hadi, 2025; Li et al., 2025; Zou et al., 2025). Specifically, blockchain's decentralized nature eliminates the need for a central authority, mitigating single points of failure and enhancing the overall resilience of the federated learning system (Jasim & Hadi, 2025; Tang et al., 2024). Furthermore, integrating blockchain with federated learning can significantly improve the security and auditability of distributed systems by enabling transparent and tamper-proof model updates, reducing the risk of adversarial attacks, and establishing immutable logs (Rane et al., 2024).

This decentralized framework addresses the security vulnerabilities of a single central server, preventing system crashes and falsified global models that could mislead training and increase resource consumption (Kang et al., 2022). This approach also bolsters the accountability of participating nodes by providing an immutable record of their contributions and model updates, which is crucial for maintaining trust and regulatory compliance in multi-party federated environments (Dutta et al., 2024; Jasim & Hadi, 2025). The cryptographic primitives inherent in blockchain, such as hash functions and asymmetric-key encryption, further bolster the security of financial transactions and data integrity across different participating nodes (Jasim & Hadi, 2025). Moreover, blockchain-based federated learning schemes enhance data provenance and traceability by recording each model update and the associated participant, thereby establishing a verifiable and auditable training procedure (Qammar et al., 2022; Zuo et al., 2024).

Cloud Computing as an Orchestration Backbone

Cloud platforms provide scalable infrastructure for federated environments, orchestrating distributed learning tasks, updating global models, and ensuring compute elasticity. They serve as a nexus between edge nodes and AI layers, enabling dynamic workload balancing, model synchronization, and continuous pipelines for data-driven innovation. Cloud-native architectures ensure adaptability, modularity, and rapid deployment of AI services within federated ecosystems. Moreover, the inherent scalability of cloud environments allows for the

efficient management of diverse computational demands, accommodating the fluctuating resource requirements of numerous edge devices participating in federated learning (Rane et al., 2024). This dynamic allocation of resources within the cloud infrastructure significantly enhances the efficiency and responsiveness of federated learning processes, allowing for rapid model aggregation and deployment across geographically dispersed IoT devices.

This integration also provides robust support for managing complex AI workflows, from data ingestion and model training to deployment and continuous monitoring, all within a secure and scalable environment (Ahmad et al., 2024). Furthermore, cloud-based orchestration facilitates the implementation of advanced security protocols and access controls, which are essential for safeguarding sensitive data and intellectual property across the distributed federated learning landscape (Pothireddy et al., 2024). The fusion of blockchain technology with cloud computing further fortifies this architecture by providing an immutable ledger for recording model updates and training parameters, thereby increasing transparency and trust in the AI development lifecycle (Jasim & Hadi, 2025). This hybrid approach leverages blockchain's cryptographic assurances and distributed consensus mechanisms to secure model updates and transactions, while simultaneously utilizing cloud computing's scalability to manage large-scale federated learning deployments (Ahmad et al., 2024). Such a synergistic integration not only enhances data integrity and verifiable governance but also offers a resilient framework against malicious attacks and unauthorized data manipulation within complex AI ecosystems (Javed et al., 2025; Singh et al., 2025).

Moreover, public-key encryption further bolsters end-to-end security in cloud environments by enabling information users to upload encrypted data using predefined access criteria, thereby securing sensitive information against related randomness attacks (Pothireddy et al., 2024). This cryptographic approach ensures that only authorized entities with the corresponding private keys can decrypt and access the data, even when stored on third-party cloud servers (Jasim & Hadi, 2025). This robust encryption methodology is critical for maintaining data confidentiality and integrity, particularly in federated learning scenarios where data ownership and privacy are paramount (Pothireddy et al., 2024). Additionally, blockchain technology, with its distributed ledger and cryptographic security features, can provide a verifiable and tamper-proof record of model updates and training parameters, significantly enhancing the trustworthiness and auditability of federated learning processes (Jasim & Hadi, 2025; Kumar et al., 2025). This distributed ledger system ensures that all transactions are recorded and replicated across the network, providing a transparent and immutable history of model evolution and contributions (Jasim & Hadi, 2025).

This combination of advanced encryption and blockchain-based auditing establishes a robust framework for secure, data-driven innovation within federated intelligence architectures (Ahmad et al., 2024). This architecture leverages blockchain's immutability to prevent malicious tampering with models, guaranteeing data integrity and enabling transparent model updates (Rane et al., 2024). Furthermore, blockchain's decentralized nature mitigates the risks associated with centralized systems, protecting against data breaches and fostering trust among participants in the federated network (Liu et al., 2024). Moreover, the adoption of blockchain technology as a decentralized, trusted-authority-free alternative bolsters the security of federated intelligence architectures by making forgeries and transaction rollbacks significantly harder, as no single entity can alter the record of any transaction (Jasim & Hadi, 2025). This inherent security feature, coupled with its ability to

maintain data integrity and provide transparent audit trails, positions blockchain as a cornerstone for developing trustworthy and resilient AI systems (Panda, 2025).

This synergy ensures that AI models are trained on verifiable data, preventing adversarial attacks and unauthorized alterations, which is critical for maintaining robust security in distributed systems (Rane et al., 2024; Samuel-Okon et al., 2024). This provides a public reference for AI models and datasets, ensuring their accessibility and verifiability by anyone through cryptographic hashes or metadata (Wang et al., 2024). The integration of blockchain also guarantees that each step in the unlearning process is immutably recorded, ensuring a verifiable and transparent certification of data removal actions crucial for auditability (Zuo et al., 2024). Such integration further solidifies trust and transparency within the federated learning ecosystem, ensuring that all participants can verify the integrity and provenance of both the data and the resulting models (Zuo et al., 2024). This immutability ensures that once data is recorded on the blockchain, any subsequent attempts to modify or tamper with it would require the consensus of the entire network, making such alterations practically impossible or infeasible (Ramos & Ellul, 2024).

This characteristic fundamentally enhances the security posture of federated intelligence architectures by establishing a transparent and unalterable record of all operations (Hayouni & Nasraoui, 2025; Li et al., 2025). This robust framework is crucial for safeguarding against data breaches and ensuring the integrity of AI models in environments where data privacy and security are paramount. The transparency offered by blockchain, through immutable records of AI operations and decision-making processes, further enhances trust by making AI outputs verifiable and auditable (Akther et al., 2025). This includes the ability to certify the unlearning process, ensuring compliance with data deletion requests and regulatory mandates (Zuo et al., 2025). Furthermore, the cryptographic linking of blocks, each containing a list of transactions and identified by cryptographic hashes, underpins the immutability and integrity of the recorded data within the blockchain (Li et al., 2025; Zuo et al., 2024). This distributed ledger technology ensures that every transaction, data input, and model adjustment is permanently recorded and verifiable, which is critical for auditability in sensitive sectors like healthcare and finance (Akther et al., 2025).

Additionally, the inherent transparency of blockchain, where all information stored is accessible to full nodes, allows for a comprehensive understanding of algorithm operations and data disclosure within a federated learning system (Cai et al., 2024). This public accessibility to the distributed ledger fosters accountability and allows for proactive identification of potential biases or anomalies in the AI models (Ramos & Ellul, 2024). Moreover, blockchain-based systems offer a decentralized alternative to traditional centralized servers, storing and aggregating local models while also tracking malicious activities (Shanmugarasa et al., 2023). This decentralized architecture significantly reduces single points of failure and enhances the overall resilience of the federated intelligence network (Jasim & Hadi, 2025). This distributed consensus mechanism ensures that all nodes agree on the validity of transactions and maintain a consistent, shared ledger (Goh et al., 2023; K.M. et al., 2024). This collective agreement among network participants is crucial for upholding data integrity and preventing unauthorized modifications, further solidifying the security of federated intelligence architectures (Jasim & Hadi, 2025).

This intrinsic security feature is further bolstered by the verifiable nature of blockchain, allowing for transparent oversight of AI system operations and data provenance (Ramos & Ellul, 2024). By recording all transactions, including consent management, data access

requests, and model updates in a tamper-evident manner, blockchain ensures traceability across the ecosystem (Nawaz et al., 2025). This level of transparency and immutability is particularly vital for regulatory compliance and fostering public trust in AI applications (Commey et al., 2024). The integration of cryptographic hashing within blockchain networks plays a pivotal role in securing these federated architectures, as exemplified by the performance benefits of algorithms like Blake3 over SHA256 in consensus mechanisms (Jasim & Hadi, 2025). Such advancements in hashing algorithms not only enhance the efficiency of blockchain operations but also contribute to the overall security and scalability of federated learning systems (Jasim & Hadi, 2025).

Security, Privacy, and Zero-Trust Governance

Federated intelligence directly addresses the cybersecurity shortcomings inherent in centralized computing. Data remains local, reducing attack surfaces, while cryptographic techniques—such as differential privacy, secure multiparty computation, and homomorphic encryption—protect model exchanges. Adopting zero-trust architectures further enforces authentication, authorization, and verification policies across nodes, mitigating threats such as model poisoning, adversarial learning, and unauthorized data extraction. This multi-layered security approach is essential for robustly defending against sophisticated cyber threats in decentralized AI environments (Alsulaimawi, 2024). Furthermore, the decentralized nature of blockchain, complemented by its transparent and tamper-proof characteristics, provides a robust framework for managing and verifying data and model integrity within these complex federated ecosystems (Jasim & Hadi, 2025; Liu et al., 2024). This integration ensures a secure and auditable infrastructure where the provenance of data and the evolution of AI models can be meticulously tracked and verified (Liu et al., 2024; Rane et al., 2024).

The incorporation of blockchain for asset tracking in federated learning environments, which distinguishes between datasets, operations, and models, extends the provenance model to address critical issues such as privacy, audibility, and fair compensation (Akbarfam & Maleki, 2024). This enables transparent tracking of data usage and intellectual property, crucial for fostering trust and incentivizing participation in data-driven innovation (Sun et al., 2024; Vyhmeister & Castañé, 2024). This advanced framework, therefore, significantly strengthens the integrity and accountability of AI development by providing an immutable record of all processes and contributions, thereby mitigating risks associated with data manipulation and intellectual property theft (Short et al., 2022; Wang et al., 2025). This comprehensive approach ensures that all participants can verify the legitimate use of their data and models, fostering an environment of trust essential for collaborative AI development (Li et al., 2025; Lo et al., 2021).

Zero-trust foundation models further elevate this security paradigm by integrating continuous verification, least privilege access, and behavioral analytics into the design and deployment of foundational models, transforming conventional trust-based IoT architectures into resilient, self-defending ecosystems (Li et al., 2025). This integration of zero-trust principles within federated learning ensures that every access request, whether for data or model parameters, is rigorously authenticated and authorized, regardless of its origin (Li et al., 2025). This continuous authentication and authorization process, coupled with AI-driven authentication mechanisms, ensures that no entity, internal or external, is implicitly trusted, thereby significantly reducing the attack surface within the federated network (Poongodi, 2025). This robust security posture is further enhanced by leveraging blockchain's immutable

ledger, which logs all access requests and model updates, creating an unalterable audit trail for accountability and compliance (Javed et al., 2025; Narkedimilli et al., 2025).

This integration provides a verifiable and tamper-proof record of all interactions within the federated intelligence architecture, reinforcing the integrity and trustworthiness of the entire system (Bonthu & Goel, 2025). The proposed blockchain-enabled federated learning framework specifically addresses the critical need for continuous monitoring and diagnosis within Zero Trust Architecture implementations, offering a robust decentralized model focused on context awareness and anomaly detection for streaming data (Pokhrel et al., 2024). This is particularly vital in IoT environments where real-time threat identification and mitigation are paramount (Pokhrel et al., 2024). Such an approach guarantees that confidential information remains on the owner's device, eliminating the need to distribute or consolidate data, directly addressing privacy concerns while ensuring secure and reliable trust computation (Pokhrel et al., 2024; Zuo et al., 2024). This method, therefore, mitigates vulnerabilities associated with centralized data storage and processing, enhancing overall system resilience against cyberattacks (Pokhrel et al., 2024).

Moreover, the integration of AI within Zero Trust Architecture extends its capabilities beyond static policies, enabling dynamic risk assessment, behavioral analytics, and real-time policy modifications to identify and mitigate unusual activities effectively (Kollipara, 2025). This includes using machine learning for intrusion detection and adaptive algorithms to bolster network resilience (Ma et al., 2025). Specifically, AI models can continually analyze behavioral patterns to refine data access controls, ensuring governance policies are upheld across complex, decentralized networks (Aden et al., 2025). Furthermore, blockchain technology bolsters these AI-driven security measures by providing an immutable ledger for recording all access requests and policy changes, thereby ensuring transparency and auditability in compliance enforcement. This synergy of AI and blockchain provides a robust mechanism for enforcing zero-trust principles, allowing for proactive identification and response to security threats by analyzing vast amounts of security data in real-time (Hasan, 2024).

This integration creates a self-healing and adaptive security ecosystem capable of responding to evolving threats with minimal human intervention, thereby significantly enhancing the overall security posture of federated intelligence architectures. This approach facilitates a continuous learning process for security policies, allowing the system to adapt to new attack vectors and maintain a high level of protection without compromising the performance or scalability of the federated network (Ajish, 2024; Hussain et al., 2024). The combined power of federated learning, blockchain, and zero-trust principles therefore offers a transformative approach to securing data-driven innovation across AI, IoT, and cloud ecosystems, enabling secure collaboration and robust defense against sophisticated cyber threats (Pokhrel et al., 2024). This synergistic framework moves beyond traditional perimeter-based security, establishing a dynamic and adaptive defense that is crucial for safeguarding sensitive data and intellectual property in an increasingly interconnected and adversarial digital landscape.

Furthermore, by embedding AI-driven threat intelligence directly into the Zero Trust architecture, organizations can proactively enhance their security posture against emerging threats (Dash, 2024). This is achieved through advanced machine learning models that detect anomalous network activities and potential phishing attempts by learning from historical attack data and adapting to new threat landscapes (Chowdhury, 2024). Such models enable

real-time detection of irregularities and facilitate the implementation of detailed authorization mechanisms, effectively preventing insider threats and sophisticated AI-based attacks (Karamchand, 2024). This integration makes the framework more adaptable by providing real-time threat detection and continuous authentication protocols, coupled with automated security responses (Karamchand, 2024). This proactive stance, supported by the integration of AI with ZTA, results in quicker reaction times, reduced human error, and the deployment of adaptive security tools designed to counter novel cyber threats (Dash, 2024; Paul et al., 2024).

This synergistic approach provides future-proof security methods to counter upcoming cyberattack patterns, as organizations require adaptive security measures to combat AI-powered cybercriminals (Karamchand, 2024). This is particularly pertinent given the increasing sophistication of adversarial AI techniques, where AI models are used to bypass traditional security defenses, necessitating an equally advanced AI-driven defensive strategy (Paul et al., 2024). The integration of AI with Zero Trust Architecture thus moves beyond merely enhancing existing security measures; it fundamentally redefines the security paradigm by embedding continuous verification and real-time threat intelligence into the core of the infrastructure (Kommera, 2025; Poongodi, 2025). This approach leverages AI's analytical capabilities to monitor network activity, identify behavioral anomalies, and predict potential threats, thereby strengthening ZTA's core principles of continuous verification and identity management (Hasan, 2024; Kommera, 2025).

Interoperability and the Emergence of Cognitive Ecosystems

The convergence of AI, IoT, and cloud technologies forms cognitive ecosystems capable of contextual understanding, autonomous adaptation, and decentralized decision-making. Federated intelligence fosters interoperability among heterogeneous devices and platforms, enabling unified operational logic without compromising autonomy. This architectural progression lays the foundations for next-generation infrastructures such as smart grids, intelligent mobility systems, and globally distributed knowledge networks. This seamless integration is vital for developing truly intelligent environments where data from disparate sources can be securely shared and processed to derive actionable insights (Bhushan et al., 2025). Moreover, the distributed nature of federated intelligence, combined with robust AI-driven security protocols, ensures that these cognitive ecosystems maintain high levels of privacy and data integrity while operating across diverse organizational and geographical boundaries (Olayinka et al., 2025).

This facilitates the creation of a resilient and scalable infrastructure essential for supporting complex AI applications and data-intensive services in a secure and efficient manner (Rangaraju, 2023; Yalla, 2024). The decentralized processing inherent in federated architectures significantly reduces single points of failure, enhancing overall system robustness and ensuring continuous availability of services even under localized disruptions. This distributed paradigm also supports enhanced scalability, allowing for the flexible integration of new devices and computational resources without compromising the integrity or performance of the overarching system (Kumaravelu, 2024). Furthermore, the interoperability standards inherent in cognitive ecosystems facilitate the seamless integration of diverse IoT devices and cloud platforms, overcoming the challenges posed by heterogeneous technologies (Ahmad et al., 2024).

These standards facilitate unified data schemas and standardized interfaces, essential for coherent decision-making across disparate environments (Obuse et al., 2025). This

evolution is crucial for unlocking the full potential of interconnected systems, transforming raw data into sophisticated, context-aware intelligence that powers autonomous operations (Arjomandi et al., 2024). This comprehensive framework thereby creates a robust foundation for the development of secure and efficient data-driven innovation across AI, IoT, and cloud ecosystems, allowing for decentralized machine learning approaches without centralizing sensitive data (Rane et al., 2024). This approach is particularly critical for fostering the "Cognitive Internet," where connected objects acquire knowledge independently and collaborate across diverse domains, moving beyond the limitations of traditional IoT paradigms (Arjomandi et al., 2024).

The architectural shift towards federated intelligence fundamentally redefines how data management, storage, and generation occur within these ecosystems, moving away from isolated, proprietary systems towards a more interconnected and cooperative framework (Friedrich et al., 2024). This facilitates the development of open platforms and reference architectures that support technological diversification and address the complex, cooperative work required for cross-industry interoperability in IoT implementations (Vermesan et al., 2022). Such a paradigm significantly enhances the utility of IoT devices, which are projected to reach 34.4 billion by 2032, by allowing them to participate in model training without requiring constant connectivity or uniform data distribution, addressing challenges like limited computational power and high latency in centralized cloud solutions (Adame et al., 2024; Ahmad et al., 2024; Rane et al., 2024). This distributed approach also inherently mitigates the risks associated with data breaches, as sensitive information remains localized and is not aggregated in a single, vulnerable cloud server (Ahmad et al., 2024).

Furthermore, the adherence to ethical guidelines and data protection regulations within these federated systems prioritizes responsible data collection and processing, ensuring user privacy and trust through transparent governance and anonymization techniques (Ahmad et al., 2024). This decentralization significantly bolsters privacy by enabling machine learning models to be trained on local data, thereby eliminating the necessity for raw data transfer to a centralized server (Ahmad et al., 2024; Yang et al., 2025). This approach significantly mitigates privacy risks and supports compliance with stringent data protection regulations by ensuring that sensitive information remains at its source (Chen et al., 2024; Deshmukh et al., 2025). This distributed privacy-preserving paradigm is especially crucial given the increasing public distrust in data-driven applications due to privacy concerns associated with centralized data pooling (Zhang et al., 2022).

Federated learning, by allowing models to be trained locally on devices and only sharing aggregated updates, inherently addresses these concerns by minimizing the exposure of sensitive data (Shirvani & Ghasemshirazi, 2024). This approach significantly lowers the risk of data breaches and aligns with data privacy regulations such as the General Data Protection Regulation by preventing the transfer of raw, sensitive information to a central server (Rane et al., 2024). This decentralized methodology offers a robust solution for ensuring data security and user privacy, which are paramount in an era where data proliferation from billions of IoT devices poses significant challenges to conventional centralized approaches (Rane et al., 2024; Shirvani & Ghasemshirazi, 2024; Zhang et al., 2022). Thus, Federated Learning has emerged as a promising paradigm to address these issues by enabling collaborative model training without requiring raw data centralization (Feng et al., 2024; Stephan et al., 2025).

This ensures that sensitive information remains on local devices, significantly reducing the potential for privacy breaches and unauthorized access, a critical advantage over traditional centralized machine learning models (Bachlechner et al., 2024; Gao et al., 2020). Specifically, in federated learning, each device trains its local model using its own data, transmitting only updated model parameters to a central server for aggregation, thereby maintaining data locality and enhancing privacy (Shen et al., 2020; Vyhmeister & Castañé, 2024). This distributed approach is particularly beneficial in contexts with stringent data protection requirements, such as healthcare, where patient confidentiality is paramount (Shahsavari et al., 2024). Moreover, this localized training paradigm minimizes the attack surface associated with centralized data processing and storage, thereby enhancing overall security (Rane et al., 2024).

CONCLUSION

This study concludes that federated intelligence architectures represent a foundational advancement for secure, privacy-preserving, and scalable data-driven innovation across AI, IoT, and cloud environments. Federated learning reduces privacy risks by ensuring data remains localized, while blockchain strengthens model integrity, auditability, and trust among distributed stakeholders. The incorporation of zero-trust principles further enhances system resilience by enforcing continuous authentication and rigorous access controls. When integrated with edge intelligence, these components significantly improve latency, bandwidth efficiency, and real-time decision-making, laying the groundwork for robust cognitive ecosystems. The findings demonstrate that such architectures not only address current challenges in security, interoperability, and governance but also open pathways for future distributed AI infrastructures capable of autonomous and context-aware operations.

LIMITATIONS AND FUTURE RESEARCH RECOMMENDATIONS

This research is limited by its qualitative and literature-based approach, which relies heavily on secondary data without empirical validation through system implementation or experimental testing. The rapidly evolving nature of federated learning, blockchain cryptography, and zero-trust security presents additional constraints, as new vulnerabilities, architectures, and regulatory requirements may emerge beyond the scope of reviewed studies. Furthermore, the analysis does not assess computational trade-offs, energy consumption, or real-world performance metrics, which are critical for deployment across heterogeneous IoT devices. Interoperability and scalability were discussed conceptually, yet practical evaluation across industry domains remains limited.

Future studies should empirically evaluate federated intelligence architectures through prototype development and cross-domain pilot testing to measure performance, energy efficiency, communication overhead, and resilience against adversarial threats. Research is also needed to design lightweight cryptographic protocols suitable for resource-constrained IoT devices, along with adaptive federated learning algorithms capable of handling extreme data heterogeneity. Integration models that combine blockchain, zero-trust authentication, and real-time anomaly detection should be explored further through simulation and real-world deployment. Additionally, interdisciplinary research examining regulatory compliance, ethical governance, and economic models for data-sharing incentives will be essential to support widespread adoption of federated intelligence ecosystems.

REFERENCES

Abbas, S., Abbas, Z., Zahir, A., & Lee, S. W. (2024). Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration [Review of Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration]. *Healthcare*, 12(24), 2587. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/healthcare12242587

Adame, T., Amri, E., Antonopoulos, G., Azaiez, S., Berne, A., Camargo, J. S., Kakoulidis, H., Kleisarchaki, S., Llamedo, A., Prasinos, M., Psara, K., & Shumaiev, K. (2024). Presenting the COGNIFOG Framework: Architecture, Building Blocks and Road toward Cognitive Connectivity. *Sensors*, 24(16), 5283. https://doi.org/10.3390/s24165283

Aden, H., Çetin, M. Ç., Chatzimisios, P., Falch, M., Ferreira, A., Gómez-Barroso, J. L., Moritz, M., Özparlak, B. O., & Kanaki, E. (2025). WG5 : Legal factors in cybersecurity for wireless systems: a vertical approach. *Research Portal Denmark*, 67.

Aggarwal, M., Khullar, V., & Goyal, N. (2024). A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training *[Review of A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training]. CRC Press eBooks*, 570. Informa. https://doi.org/10.1201/9781003471059-73

Ahmad, W., Almaiah, M. A., Ali, B. S., & Ali, A. (2024). A Privacy Preserving Federated Learning BasedIoT Framework Using Cloud Computing. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-4701071/v1

Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: a comprehensive review *[Review of The significance of artificial intelligence in zero trust technologies: a comprehensive review]. Journal of Electrical Systems and Information Technology*, 11(1). Springer Science+Business Media. https://doi.org/10.1186/s43067-024-00155-z

Akbarfam, A. J., & Maleki, H. (2024). SOK: Blockchain for Provenance. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2407.17699

Akther, A., Arobee, A., Adnan, A. A., Auyon, O., Islam, A. J., & Akter, F. (2025). Blockchain As a Platform For Artificial Intelligence (AI) Transparency. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2503.08699

Albelaihi, R. (2025). Mobility Prediction and Resource-Aware Client Selection for Federated Learning in IoT. *Future Internet*, 17(3), 109. https://doi.org/10.3390/fi17030109

Albshaier, L., Almarri, S., & Albuali, A. (2025). Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities [Review of Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities]. Electronics, 14(5), 1019. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/electronics14051019

Alsulaimawi, Z. (2024). *Securing Federated Learning with Control-Flow Attestation: A Novel Framework for Enhanced Integrity and Resilience against Adversarial Attacks*. https://doi.org/10.48550/ARXIV.2403.10005

Arjomandi, F., Alamouti, S., Burger, M., & Altakrouri, B. (2024). Building Blocks to Empower Cognitive Internet with Hybrid Edge Cloud. In *Lecture notes in networks and systems* (p. 534). Springer International Publishing. https://doi.org/10.1007/978-3-031-73125-9_34

Bachlechner, D., Hetfleisch, R. H., Krenn, S., Lorünser, T., & Rader, M. (2024). Protecting Privacy in Federated Time Series Analysis: A Pragmatic Technology Review for Application Developers. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2408.15694

Barbosa, A. V., Ngo, T. B. T., Jafarigol, E., Trafalïs, T. B., & Ojoboh, E. P. (2025). Using Federated Machine Learning in Predictive Maintenance of Jet Engines. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2502.05321

Barros, A., Veiga, R., Morais, R., Rosário, D., & Cerqueira, E. (2024). MESFLA: Model Efficiency through Selective Federated Learning Algorithm. *Journal of Internet Services and Applications*, 15(1), 495. https://doi.org/10.5753/jisa.2024.4044

Beltrán, E. T. M., Gómez, Á. L. P., Feng, C., Sánchez, P. M. S., Bernal, S. L., Bovet, G., Pérez, M. G., Pérez, G. M., & Celdrán, A. H. (2023). Fedstellar: A Platform for Decentralized Federated Learning. *Expert Systems with Applications*, 242, 122861. https://doi.org/10.1016/j.eswa.2023.122861

Bhushan, B., Rajgopal, P. R., & Sharma, K. C. (2025). An Intent-Aware Zero Trust Identity Architecture for Unifying Human and Machine Access. *International Journal of Computational and Experimental Science and Engineering*, 11(3). https://doi.org/10.22399/ijcesen.3886

Bonthu, C., & Goel, G. (2025). Autonomous Supplier Evaluation and Data Stewardship with AI: Building Transparent and Resilient Supply Chains. *International Journal of Computational and Experimental Science and Engineering*, 11(3). https://doi.org/10.22399/ijcesen.3854

Boruga, D., Bolintineanu, D., & Racates, G. I. (2024). Federated learning in edge computing: Enhancing data privacy and efficiency in resource-constrained environments. *World Journal of Advanced Engineering Technology and Sciences*, 13(2), 205. https://doi.org/10.30574/wjaets.2024.13.2.0563

Cai, Z., Chen, J., Fan, Y., Zheng, Z., & Li, K. (2024). Blockchain-empowered Federated Learning: Benefits, Challenges, and Solutions. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2403.00873

Campos, E. M., González-Vidal, A., Hernández-Ramos, J. L., & Skármeta, A. (2024). FedRDF: A Robust and Dynamic Aggregation Function against Poisoning Attacks in Federated Learning. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.10082

Cheikh, I., Roy, S., Sabir, E., & Aouami, R. (2025). Energy, Scalability, Data and Security in Massive IoT: Current Landscape and Future Directions. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2505.03036

Chen, C., Liu, J., Tan, H., Li, X., Wang, K. I., Li, P., Sakurai, K., & Dou, D. (2024). Trustworthy federated learning: privacy, security, and beyond. *Knowledge and Information Systems*, 67(3), 2321. https://doi.org/10.1007/s10115-024-02285-2

Chowdhury, R. H. (2024). Blockchain and AI: Driving the future of data security and business intelligence. *World Journal of Advanced Research and Reviews*, 23(1), 2559. https://doi.org/10.30574/wjarr.2024.23.1.2273

Commey, D., Hounsinou, S., & Crosby, G. V. (2024). Securing Health Data on the Blockchain: A Differential Privacy and Federated Learning Framework. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2405.11580

Dash, B. (2024). Zero-Trust Architecture (ZTA): *Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems*. 4(2), 1. https://doi.org/10.54026/ctes/1058

Deshmukh, A., Rosa, J. L. de la, Rodriguez, R. V., & Dasari, S. (2025). Enhancing Privacy in IoT-Enabled Digital Infrastructure: Evaluating Federated Learning for Intrusion and Fraud Detection. *Sensors*, 25(10), 3043. https://doi.org/10.3390/s25103043

Dhinakaran, D., Sankar, S. M. U., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2401.00794

Dutta, S., Freitas, I. L. de, Xavier, P. M., Farias, C. M. de, & Bernal, D. E. (2024). Federated Learning in Chemical Engineering: A Tutorial on a Framework for Privacy-Preserving Collaboration Across Distributed Data Sources. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.16737

Erdal, Ş., Karakoç, F., & Ozdemır, E. (2024). A Survey On Security and Privacy Aspects and Solutions for Federated Learning in Mobile Communication Networks. *DergiPark (Istanbul University)*. https://dergipark.org.tr/tr/pub/itujwcc/issue/87385/1482654

Feng, C., Celdrán, A. H., Assen, J. von der, Beltrán, E. T. M., Bovet, G., & Stiller, B. (2024). DART: A Solution for decentralized federated learning model robustness analysis. *Array*, 23, 100360. https://doi.org/10.1016/j.array.2024.100360

Friedrich, C., Vogt, S., Rudolph, F. B., Patolla, P., Grützmann, J. M., Hohmeier, O., Richter, M., Wenzel, K., Reichelt, D., & Ihlenfeldt, S. (2024). Enabling Federated Learning Services Using OPC UA, Linked Data and GAIA-X in Cognitive Production. *Journal of Machine Engineering*, 24(2), 18. https://doi.org/10.36897/jme/188618

Gao, Y., Kim, M., Abuadbba, A., Kim, Y., Thapa, C., Kim, K., Camtep, S. A., Kim, H., & Nepal, Surya. (2020). *End-to-End Evaluation of Federated Learning and Split Learning for Internet of Things*. https://doi.org/10.1109/srds51746.2020.00017

Garg, M. (2025). Adaptive Differential Privacy in Federated Edge AI for Medical IoT: Energy-Efficient, HIPAA-Compliant Frameworks for Distributed Real-Time Diagnostics. *Journal of Information Systems Engineering & Management*, 10, 36. https://doi.org/10.52783/jisem.v10i34s.5773

Goh, E., Kim, D., Kim, D.-Y., & Lee, K. (2023). Blockchain-Enabled Federated Learning: A Reference Architecture Design, Implementation, and Verification. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2306.10841

Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2410.18291

Hayouni, H., & Nasraoui, L. (2025). NAIDS4IoT: A Novel Artificial Intelligence-Based Intrusion Detection Architecture for the Internet of Things. *Inteligencia Artificial*, 28(76), 253. https://doi.org/10.4114/intartif.vol28iss76pp253-282

Himeur, Y., Sayed, A. N., Alsalemi, A., Bensaali, F., & Amira, A. (2023). Edge AI for Internet of Energy: Challenges and perspectives. *Internet of Things*, 25, 101035. https://doi.org/10.1016/j.iot.2023.101035

Huang, H., Iskandarov, B., Rahman, M., Otal, H. T., & Canbaz, M. A. (2024). Federated Learning in Adversarial Environments: Testbed Design and Poisoning Resilience in Cybersecurity. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2409.09794

Hussain, M., Pal, S., Jadidi, Z., Foo, E., & Kanhere, S. S. (2024). Federated Zero Trust Architecture using Artificial Intelligence. *IEEE Wireless Communications*, 31(2), 30. https://doi.org/10.1109/mwc.001.2300405

Jasim, Z. A., & Hadi, A. K. (2025). Optimizing Blockchain Network Performance Using Blake3 Hash Function in POS Consensus Algorithm. *IEEE Access*, 1. https://doi.org/10.1109/access.2025.3546723

Javed, F., Zeydan, E., Mangues-Bafalluy, J., Dev, K., & Blanco, L. (2025). Blockchain for Federated Learning in the Internet of Things: Trustworthy Adaptation, Standards, and the Road Ahead. *IEEE Communications Standards Magazine*, 1. https://doi.org/10.1109/mcomstd.2025.3593809

Kang, J., Xiong, Z., Jiang, C., Liu, Y., Guo, S., Zhang, Y., Niyato, D., Leung, C., & Miao, C. (2022). Scalable and Communication-efficient Decentralized Federated Edge Learning with Multi-blockchain Framework. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2008.04743

Karamchand, G. (2024). Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation. *World Journal of Advanced Research and Reviews*, 24(3), 3374. https://doi.org/10.30574/wjarr.2024.24.3.3883

K.M., S., Nicolazzo, S., Arazzi, M., Nocera, A., A., R. R. K., Vinod, P., & Conti, M. (2024). Privacy-preserving in Blockchain-based Federated Learning systems. *Computer Communications*, 222, 38. https://doi.org/10.1016/j.comcom.2024.04.024

Kollipara, Y. V. P. (2025). Zero Trust Architecture in Mission-Critical Systems: From Perimeter Security to Continuous Verification. *Journal of Information Systems Engineering & Management*, 10, 251. https://doi.org/10.52783/jisem.v10i61s.13351

Kommera, S. (2025). Enhancing Zero Trust Architecture with AI-Driven Threat Intelligence in Cloud Environments. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 11(1), 1524. https://doi.org/10.32628/cseit251112163

Kumar, M., Samriya, J. K., Walia, G. K., Verma, P., Wu, H., & Gill, S. S. (2025). Blockchain Empowered Secure Federated Learning for Consumer IoT Applications in Cloud-Edge Collaborative Environment. *IEEE Transactions on Consumer Electronics*, 71(2), 3986. https://doi.org/10.1109/tce.2025.3532676

Kumar, S., Vahabi, M., & Fotouhi, H. (2025). Federated learning at the edge in Industrial Internet of Things: A review [Review of Federated learning at the edge in Industrial Internet of Things: A review]. *Sustainable Computing Informatics and Systems*, 46, 101087. Elsevier BV. https://doi.org/10.1016/j.suscom.2025.101087

Kumaravelu, A. (2024). Leveraging AI for Enhanced IT Infrastructure: An Examination of Automated Processes and Their Impacts. *International Journal for Research in Applied Science and Engineering Technology*, 12(9), 10. https://doi.org/10.22214/ijraset.2024.64036

Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., Ni, W., Niyato, D., Jamalipour, A., Dressler, F., & Akan, Ö. B. (2025). Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *IEEE Internet of Things Journal*, 1. https://doi.org/10.1109/jiot.2025.3603957

Li, M., Wang, M., & Duan, M. (2025). Atomic and privacy-preserving cyclic cross-chain protocol based on chameleon hash function. *Blockchain Research and Applications*, 100262. https://doi.org/10.1016/j.bcra.2024.100262

Li, W., Hacid, H., Almazrouei, E., & Debbah, M. (2023). A Comprehensive Review and a Taxonomy of Edge Machine Learning: Requirements, Paradigms, and Techniques *[Review of A Comprehensive Review and a Taxonomy of Edge Machine Learning: Requirements,*

Paradigms, and Techniques]. AI, 4(3), 729. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/ai4030039

Lin, H.-T., & Wen, C.-Y. (2024). Edge Federated Optimization for Heterogeneous Data. *Future Internet*, 16(4), 142. https://doi.org/10.3390/fi16040142

Liu, J., Chen, C., Li, Y., Sun, L., Song, Y., Zhou, J., Jing, B., & Dou, D. (2024a). Enhancing Trust and Privacy in Distributed Networks: A Comprehensive Survey on Blockchain-based Federated Learning. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2403.19178

Liu, J., Chen, C., Li, Y., Sun, L., Song, Y., Zhou, J., Jing, B., & Dou, D. (2024b). Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. *Knowledge and Information Systems*, 66(8), 4377. https://doi.org/10.1007/s10115-024-02117-3

Lo, S. K., Lu, Q., Wang, C., Paik, H.-Y., & Zhu, L. (2021). A Systematic Literature Review on Federated Machine Learning [*Review of A Systematic Literature Review on Federated Machine Learning]. ACM Computing Surveys*, 54(5), 1. Association for Computing Machinery. https://doi.org/10.1145/3450288

Ma, X., Fang, F., & Wang, X. (2025). Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.03601

Madathil, N. T., Dankar, F. K., Gergely, M., Belkacem, A. N., & Alrabaee, S. (2025). Revolutionizing Healthcare Data Analytics with Federated Learning: A Comprehensive Survey of Applications, Systems, and Future Directions [*Review of Revolutionizing Healthcare Data Analytics with Federated Learning: A Comprehensive Survey of Applications, Systems, and Future Directions]. Computational and Structural Biotechnology Journal*, 28, 217. Elsevier BV. https://doi.org/10.1016/j.csbj.2025.06.009

Mahmood, K., Khan, S., Abdelhaq, M., Hassan, M. ul, Uddin, M., Alsaqour, R., Awan, K. A., & Alsoufi, M. A. (2025). Adaptive resource aware and privacy preserving federated edge learning framework for real time internet of medical things applications. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-23398-w

Marengo, A. (2024). Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms [Review of Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms]. *Internet of Things*, 27, 101318. Elsevier BV. https://doi.org/10.1016/j.iot.2024.101318

Monteiro, D., Mavinkurve, I., Kambli, P., & Surve, Prof. S. (2024). Federated Learning for Privacy-Preserving Machine Learning: Decentralized Model Training with Enhanced Data Security. *International Journal for Research in Applied Science and Engineering Technology*, 12(11), 355. https://doi.org/10.22214/ijraset.2024.65062

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

Munusamy, S., & Jothi, K. (2025a). 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

Munusamy, S., & Jothi, K. R. (2025b). Blockchain-Enabled Federated Learning with Edge Analytics for Secure and Efficient Electronic Health Records Management. *Research Square*. https://doi.org/10.21203/rs.3.rs-6678464/v1

Narkedimilli, S., Sriram, A., Makam, S., Sathvik, M., & Mallellu, S. P. (2025). FAPL-DM-BC: A Secure and Scalable FL Framework with Adaptive Privacy and Dynamic Masking, Blockchain, and XAI for the IoVs. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.01063

Narkedimilli, S., Sriram, A., & Raghav, S. (2024). FL-DABE-BC: A Privacy-Enhanced, Decentralized Authentication, and Secure Communication for Federated Learning Framework with Decentralized Attribute-Based Encryption and Blockchain for IoT Scenarios. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2410.20259

Nawaz, A., Irfan, M., Yu, X., Zou, Z., & Westerlund, T. (2025). Blockchain-Enabled Privacy-Preserving Second-Order Federated Edge Learning in Personalized Healthcare. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2506.00416

Nori, M. K., Yun, S., & Kim, I. (2021). Fast Federated Learning by Balancing Communication Trade-Offs. *IEEE Transactions on Communications*, 69(8), 5168. https://doi.org/10.1109/tcomm.2021.3083316

Obuse, E., Ayanbode, N., Cadet, E., Essien, I. A., & Etim, E. D. (2025). Privacy-First security models for AI-integrated identity governance in multi-access cloud and edge environments. *Computer Science & IT Research Journal*, 6(8), 506. https://doi.org/10.51594/csitrj.v6i8.2012

Ogunbajo, A., Taiwo, I., Abidola, A. Q., Adediran, O. F., & Agbo-Adediran, I. (2025). Privacy preserving AI models for decentralized data management in federated information systems. *GSC Advanced Research and Reviews*, 22(2), 104. https://doi.org/10.30574/gscarr.2025.22.2.0043

Olagunju, F. (2025). Federated Learning in the Era of Data Privacy: An Exhaustive Survey of Privacy Preserving Techniques, Legal Frameworks, and Ethical Considerations. *International Journal of Future Engineering Innovations*, 2(3), 153. https://doi.org/10.54660/ijfei.2025.2.3.153-160

Olayinka, O. T., Jeswani, S., & Iloh, D. (2025). Adaptive Cybersecurity Architecture for Digital Product Ecosystems Using Agentic AI. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2509.20640

Otoum, Y., Asad, A., & Nayak, A. (2025). *LLMs meet Federated Learning for Scalable and Secure IoT Management*. https://doi.org/10.48550/ARXIV.2504.16032

Panda, S. N. (2025). *Blockchain Technologies for Secure and Transparent Artificial Intelligence Systems*. https://doi.org/10.2139/ssrn.5250372

Paul, É., Paul, É., Kessie, J. D., & Salawudeen, M. D. (2024). Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks. *International Journal of Science and Research Archive*, 13(2), 4159. https://doi.org/10.30574/ijsra.2024.13.2.2583

Pokhrel, S. R., Yang, L., Rajasegarar, S., & Li, G. (2024a). Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.17172

Pokhrel, S. R., Yang, L., Rajasegarar, S., & Li, G. (2024b). *Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework*. 7. https://doi.org/10.1145/3672200.3673878

Poongodi, R. K. (2025). Zero Trust AI Authentication and Blockchain Powered Secure AI. *International Journal for Research in Applied Science and Engineering Technology*, 13(2), 52. https://doi.org/10.22214/ijraset.2025.66800

Pothireddy, S., Peddisetty, N., Yellamma, P., Botta, G., & Kailash, N. (2024). Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability. *International Journal of Intelligent Engineering and Systems*, 17(2), 159. https://doi.org/10.22266/ijies2024.0430.14

Puppala, S., Hossain, I., Alam, Md. J., Talukder, S., Ferdaus, J., Hasan, M., Pisupati, S., & Mathukumilli, S. (2024). Generative AI like ChatGPT in Blockchain Federated Learning: use cases, opportunities and future. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2407.18358

Qammar, A., Karim, A., Ning, H., & Ding, J. (2022). Securing federated learning with blockchain: a systematic literature review. *Artificial Intelligence Review*, 56(5), 3951. https://doi.org/10.1007/s10462-022-10271-9

Rahman, R. (2025). Federated Learning: A Survey on Privacy-Preserving Collaborative Intelligence. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2504.17703

Rahmati, M. (2025). *Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities*. https://doi.org/10.48550/ARXIV.2502.10599

Ramos, S., & Ellul, J. (2024). Blockchain for Artificial Intelligence (AI): enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. *International Cybersecurity Law Review*, 5(1), 1. https://doi.org/10.1365/s43439-023-00107-9

Rane, J., Kaya, Ö., Mallick, S. K., & Rane, N. L. (2024). *Federated learning for edge artificial intelligence: Enhancing security, robustness, privacy, personalization, and blockchain integration in IoT*. https://doi.org/10.70593/978-81-981271-0-5_3

Rangaraju, S. (2023). Secure By Intelligence: Enhancing Products with Ai-Driven Security Measures. EPH - *International Journal of Science And Engineering*, 9(3), 36. https://doi.org/10.53555/ephijse.v9i3.212

Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bağcı, U., Rawat, D. B., & Vlassov, V. (2023). Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions. *IEEE Internet of Things Journal*, 11(5), 7374. https://doi.org/10.1109/jiot.2023.3329061

Robai, M. P. (2024). Federated learning for secure and privacy preserving data analytics in heterogeneous networks. *GSC Advanced Research and Reviews*, 21(2), 527. https://doi.org/10.30574/gscarr.2024.21.2.0451

Sammangi, H., Jagatha, A., Bojja, G. R., & Liu, J. (2025). Decentralized AI-driven IoT Architecture for Privacy-Preserving and Latency-Optimized Healthcare in Pandemic and Critical Care Scenarios. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2507.15859

Samuel-Okon, A. D., Olateju, O. O., Okon, S. U., Olaniyi, O. O., & Igwenagu, U. T. I. (2024). Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence. *Archives of Current Research International*, 24(5), 612. https://doi.org/10.9734/acri/2024/v24i5735

Sánchez, O. T., Borges, G. A., Raposo, D., Rodrigues, A., Boavida, F., & Silva, J. S. (2025). Federated Learning Framework for LoRaWAN-Enabled IIoT Communication: A Case Study. *IEEE Internet of Things Journal*, 12(13), 24944. https://doi.org/10.1109/jiot.2025.3558560

Schwermer, R., Mayer, R., & Jacobsen, H. (2024a). Federated Computing -- Survey on Building Blocks, Extensions and Systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2404.02779

Schwermer, R., Mayer, R., & Jacobsen, H.-A. (2024b). Federated Computing -- Survey on Building Blocks, Extensions and Systems. https://doi.org/10.48550/ARXIV.2404.02779

Sen, J., Waghela, H., & Rakshit, S. (2024). Privacy in Federated Learning. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2408.08904

Shahsavari, Y., Dambri, O. A., Baseri, Y., Hafid, A., & Makrakis, D. (2024). Integration of Federated Learning and Blockchain in Healthcare: A Tutorial. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2404.10092

Shanmugarasa, Y., Paik, H.-Y., Kanhere, S. S., & Zhu, L. (2023). A systematic review of federated learning from clients' perspective: challenges and solutions [*Review of A systematic review of federated learning from clients' perspective: challenges and solutions]. Artificial Intelligence Review*, 56, 1773. Springer Science+Business Media. https://doi.org/10.1007/s10462-023-10563-8

Shen, S., Zhu, T., Wu, D., Wang, W., & Zhou, W. (2020). From distributed machine learning to federated learning: In the view of data privacy and security. *Concurrency and Computation Practice and Experience*, 34(16). https://doi.org/10.1002/cpe.6002

Shirvani, G., & Ghasemshirazi, S. (2024). Powering the Future of IoT: Federated Learning for Optimized Power Consumption and Enhanced Privacy. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2405.03065

Short, J. E., Miyachi, K., Toouli, C., & Todd, S. (2022). A field test of a federated learning/federated analytic blockchain network implementation in an HPC environment. *Frontiers in Blockchain*, 5. https://doi.org/10.3389/fbloc.2022.893747

Singh, J., Bharany, S., Rani, S., Rehman, A. U., Taye, B. M., Pant, R., & Kaur, U. (2025). A Systematic Review of Blockchain, AI, and Cloud Integration for Secure Digital Ecosystems. *The International Journal of Networked and Distributed Computing*, 13(2). https://doi.org/10.1007/s44227-025-00072-1

Stephan, T., Paramana, P. P. D., Lin, C., Agarwal, S., & Verma, R. (2025). Federated learning-driven IoT system for automated freshness monitoring in resource-constrained vending carts. *Journal of Big Data*, 12(1). https://doi.org/10.1186/s40537-025-01063-3

Sumanth, N., Heggere, S. B., Prathiksha, E., Shetty, C. A., Nikhitha, H. R., & Soundarya, B. C. (2023). Federated Learning: Healthcare, Security, Challenges, and Threats. *Research Square*. https://doi.org/10.21203/rs.3.rs-3223963/v1

Sun, N. X., Miao, Y., Jiang, H., Ding, M. D., & Zhang, J. (2024). From Principles to Practice: A Deep Dive into AI Ethics and Regulations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2412.04683

Tang, Y., Wang, K., Niyato, D., Chen, W., & Karagiannidis, G. K. (2024). Digital Twin-Assisted Federated Learning with Blockchain in Multi-tier Computing Systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.02323

Thomas, S. G., & Myakala, P. K. (2025). Beyond the Cloud: Federated Learning and Edge AI for the Next Decade. *Journal of Computer and Communications*, 13(2), 37. https://doi.org/10.4236/jcc.2025.132004

Uddin, M. R., Shankar, G., Mukta, S. H., Kumar, P., & Islam, A. K. M. N. (2024). Evolving Topics in Federated Learning: Trends, and Emerging Directions for IS. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2409.15773

Uddoh, J., Ajiga, D., Okare, B. P., & Aduloju, T. D. (2021). AI-Based Threat Detection Systems for Cloud Infrastructure: Architecture, Challenges, and Opportunities. Journal of *Frontiers in Multidisciplinary Research*, 2(2), 61. https://doi.org/10.54660/.ijfmr.2021.2.2.61-67

Vermesan, O., Eisenhauer, M., Sundmaeker, H., Guillemin, P., Serrano, M., Τράγος, H., Valiño, J., derWees, A. van, Gluhak, A., & Bahr, R. (2022). *Internet of Things Cognitive Transformation Technology Research Trends and Applications*. In River Publishers eBooks (p. 17). https://doi.org/10.1201/9781003337584-3

Vyhmeister, E., & Castañé, G. G. (2024). When Industry meets Trustworthy AI: A Systematic Review of AI for Industry 5.0 [Review of When Industry meets Trustworthy AI: A Systematic Review of AI for Industry 5.0]. *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2403.03061

Wang, Y., Li, Y., & Chang, X. (2025). AI Scaling: From Up to Down and Out. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2502.01677

Wang, Z., Sun, R., Lui, E., Shah, V. H., Xiong, X., Sun, J., Crapis, D., & Knottenbelt, W. J. (2024). SoK: Decentralized AI (DeAI). *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.17461

Wu, Z., Sun, S., Wang, Y., Liu, M., Xu, K., Pan, Q., Gao, B., & Tian, W. (2025). Beyond Model Scale Limits: End-Edge-Cloud Federated Learning with Self-Rectified Knowledge Agglomeration. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.00693

Yalla, M. R. (2024). Zero-trust security architecture in the ai era: a novel framework for enterprise cyber resilience. *International Journal of Science and Research Archive*, 13(2), 4341. https://doi.org/10.30574/ijsra.2024.13.2.0172

Yang, H. W., Liu, H., Yuan, X., Wu, K., Ni, W., Zhang, J. A., & Liu, R. P. (2025). Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and Federated Learning in Advanced Networked Systems [Review of Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and Federated Learning in Advanced Networked Systems]. *Applied Sciences*, 15(12), 6587. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/app15126587

Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, A. S. (2022a). Federated Learning for the Internet of Things: Applications, Challenges, and Opportunities. *IEEE Internet of Things Magazine*, 5(1), 24. https://doi.org/10.1109/iotm.004.2100182

Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B., & Avestimehr, S. (2022b). Federated Learning for Internet of Things: Applications, Challenges, and Opportunities. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2111.07494

Zhang, T., He, C., Ma, T., Gao, L., Ma, M., & Avestimehr, S. (2021). *Federated Learning for Internet of Things*. 413. https://doi.org/10.1145/3485730.3493444

Zhao, J., Bagchi, S., Avestimehr, A. S., Chan, K., Chaterji, S., Dimitriadis, D., Li, J., Li, N., Nourian, A., & Roth, H. R. (2025). The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape [Review of The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape]. *ACM Computing Surveys*, 57(9), 1. Association for Computing Machinery. https://doi.org/10.1145/3724113

Zhu, H., Huang, L., & Xie, Z. (2024). Privacy Attack in Federated Learning is Not Easy: An Experimental Study. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2409.19301

Zou, Y. L., Kuek, F., Feng, W., & Cheng, X. (2025). Digital learning in the 21st century: trends, challenges, and innovations in technology integration. *Frontiers in Education*, 10. https://doi.org/10.3389/feduc.2025.1562391

Zuo, X., Wang, M., Zhu, T., Zhang, L., Ye, D., Yu, S., & Zhou, W. (2024). Federated TrustChain: Blockchain-Enhanced LLM Training and Unlearning. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.04076

Zuo, X., Wang, M., Zhu, T., Zhang, L., Yu, S., & Zhou, W. (2024). Federated Learning with Blockchain-Enhanced Machine Unlearning: A Trustworthy Approach. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2405.20776

Zuo, X., Wang, M., Zhu, T., Zhang, L., Yu, S., & Zhou, W. (2025). Federated Learning with Blockchain-Enhanced Machine Unlearning: A Trustworthy Approach. *IEEE Transactions on Services Computing*, 1. https://doi.org/10.1109/tsc.2025.3553709