JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

A Federated Architecture for Enhancing Security and Scalability in IoT-Cloud Integrated Systems

Abdulmajeed Adil Yazdeen [1], Hewa Majeed Zangana [2*]
[1] ITM Dept., Technical College of Administration, Duhok Polytechnic University, Duhok, Iraq
[2] Duhok Polytechnic University, Duhok, Iraq
[2*] hewa.zangana@dpu.edu.krd

Keywords:
Cloud Computing, Federated Learning, IoT Security, Scalability, System Architecture.

Abstract

The exponential growth of the Internet of Things (IoT) and its integration with cloud computing has introduced significant challenges related to security, scalability, and data privacy. This paper proposes a novel federated architecture that leverages federated learning and distributed security mechanisms to enhance the resilience and scalability of IoT-cloud integrated systems. By decentralizing data processing and security enforcement, the architecture mitigates common attack vectors such as centralized point-of-failure, data leakage, and unauthorized access. The proposed system is designed with modular security components including lightweight encryption, dynamic trust management, and blockchain-inspired audit trails. A performance evaluation conducted through simulated environments and real-world IoT testbeds demonstrates improved latency, resource efficiency, and defense against cyber threats when compared to conventional centralized systems. This research contributes to the advancement of secure and scalable IoT-cloud infrastructures and offers a viable path for industrial and smart city deployments.

1.INTRODUCTION

The convergence of Internet of Things (IoT) and cloud computing has revolutionized the digital landscape, enabling real-time data collection, remote monitoring, and intelligent decision-making across domains such as healthcare, transportation, industry, and smart cities [1], [2]. However, this integration also introduces serious challenges in terms of security, scalability, and data sovereignty, which are exacerbated by the distributed and heterogeneous nature of IoT environments [3], [4].

Cloud-based IoT systems typically rely on centralized architectures, which present a single point of failure and create bottlenecks in performance, particularly under high-load conditions or in latency-sensitive applications [5], [6]. Furthermore, data offloading to cloud environments raises serious privacy concerns, especially in critical sectors like healthcare and smart governance [7], [8].

Existing IoT-cloud architectures often struggle with:

- Centralized data processing that hampers scalability.
- Weaknesses in end-to-end security and privacy assurance.
- Inflexible interoperability across heterogeneous IoT domains.
- Delayed responsiveness in real-time applications.

While traditional cloud-centric models offer robust computational capabilities, they lack the adaptability and distributed control mechanisms required to secure and scale modern IoT systems [9],

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

[10]. Furthermore, efforts to retrofit security mechanisms after deployment often result in fragmented solutions [11], [12].

To address the aforementioned challenges, this research introduces a Federated Architecture that integrates federated learning, distributed trust management, and blockchain-enabled auditing within a modular, scalable IoT-cloud framework. The primary objectives are:

- To develop a decentralized IoT-cloud integration architecture that enhances system scalability and performance.
- To ensure secure data exchange through privacy-preserving mechanisms using federated learning and lightweight encryption.
- To design a dynamic trust evaluation system leveraging semantic interoperability and blockchain for auditability and tamper resistance.
- To validate the proposed framework through simulations and real-world IoT testbeds.

The key contributions of this research are:

1. A federated, modular design that minimizes reliance on central cloud services and supports edge/fog coordination.
2. A hybrid trust mechanism combining reputation scoring and cryptographic assurance for resilient authentication.
3. An interoperable communication layer designed to support semantic integration across heterogeneous IoT platforms [13], [14].
4. A comprehensive performance evaluation demonstrating superior scalability, latency reduction, and enhanced security over existing models.

Unlike prior frameworks that focus solely on federated learning or cloud enhancements in isolation, the proposed method synthesizes multiple security and architectural paradigms into a single, coherent system. It extends the concepts of federated learning [15], [16], distributed ledgers [17], [18], and edge-cloud orchestration [19], [20] into a federated cloud-IoT security framework optimized for both scalability and privacy. Moreover, the system introduces a novel interoperability-aware trust scoring model that can operate across disparate IoT ecosystems without requiring intrusive data access.

1.1 Research Objectives

The primary objectives of this research are as follows:

1. To develop a decentralized IoT-cloud integration architecture that enhances system scalability and performance.
2. To ensure secure data exchange through privacy-preserving mechanisms using federated learning and lightweight encryption.
3. To design a dynamic trust evaluation system leveraging semantic interoperability and blockchain for auditability and tamper resistance.
4. To validate the proposed framework through simulations and real-world IoT testbeds.

2.LITERATURE REVIEW

The integration of cloud computing with the Internet of Things (IoT) has sparked significant scholarly attention due to its potential in enabling scalable, secure, and intelligent systems across domains like healthcare, smart cities, and industrial IoT. This review synthesizes the state-of-the-art advancements and research challenges across cloud-IoT convergence, focusing on security, privacy, scalability, and architectural innovations.

Federated cloud and IoT systems have emerged to support decentralized, low-latency applications. [10] introduced an early framework combining cloud and IoT for pervasive patient monitoring. Building on this, [4], [19] examined fog and edge extensions to enhance scalability and responsiveness. Huaranga-Junco et al. (2024) later compared traditional cloud, fog, and federated-fog models in real-time IoT settings, highlighting semantic interoperability as a key enabler.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

Security and privacy have remained persistent concerns in integrated architectures. [9] provided a critical analysis of protocols to secure distributed cloud environments, while [11], [21] proposed lightweight virtualization and end-to-end security designs tailored for federated cloud-IoT networks. [12] explored the fusion of trust and reputation mechanisms to enhance the dependability of cloud services in IoT environments.

Recent advancements emphasize privacy-preserving intelligence using federated learning and blockchain. [7], [8], [16] developed frameworks merging cryptography, blockchain, and federated learning to secure sensitive medical and sensor data. Similarly, [15], [22] proposed hybrid systems leveraging dense neural networks and blockchain to improve privacy in distributed IoT applications. The use of blockchain for federated learning was further extended in SecureChainAI by [18], integrating AI to boost adaptive threat detection.

Multiple works have emphasized the need for scalable architectures. [6] proposed a green, scalable healthcare framework based on cloud and IoT integration. [23] conducted a systematic review of parallel and distributed processing strategies in hybrid cloud-fog environments. [1], [20] addressed data-intensive and smart city applications, respectively, focusing on hybrid and layered infrastructure models.

Blockchain's integration with cloud-IoT is gaining momentum as demonstrated by [5], [17], who proposed distributed blockchain-SDN models for enhanced security. [24] emphasized the role of provenance and federated learning in blockchain-managed health IoT systems. The conceptual model by [25] incorporating quantum computing and 6G technologies underlines the evolving vision for future-proof federated IoT networks.

From a software and platform perspective, [2] identified integration challenges and applications of IoT cloud platforms, whereas [26] focused on enhancing network-level security in cloud-integrated IoT systems. [3] provided a comprehensive survey on the overarching security challenges and future research directions in IoT-cloud integration.

Interoperability across diverse IoT/cloud domains remains a significant hurdle. [13] tackled this by introducing the FIESTA-IoT framework based on federated semantic testbeds, promoting cross-domain operability. Similarly, the study by [11] supported lightweight NFV and standardized interfaces for federated cloud deployments.

To summarize, while cloud-IoT integration has enabled intelligent, decentralized systems, ongoing research emphasizes the importance of privacy, secure architecture, real-time processing, and cross-platform interoperability. Future directions include incorporating quantum technologies [25], enhancing parallelism [23], and leveraging semantic frameworks [13] to realize robust, scalable, and secure next-generation IoT ecosystems.

3.METHOD

This research adopts a hybrid methodological framework integrating system design, algorithm development, and security modeling to enable secure, scalable, and interoperable communication across IoT devices using federated cloud infrastructure. The method is structured into five key components:

3.1. System Architecture Design

The proposed architecture is a multi-layered federated cloud-IoT framework consisting of the following tiers:

- IoT Layer: Sensors and edge devices collect and transmit real-time data.
- Edge/Fog Layer: Performs preliminary data filtering, privacy-preserving feature extraction, and local processing to reduce latency and network load.
- Federated Cloud Layer: Distributes model training across multiple cloud environments without sharing raw data.
- Blockchain Integration Layer: Ensures data integrity, consensus, and tamper-proof logs using a lightweight blockchain framework.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

- Security Layer: Implements federated learning (FL), homomorphic encryption (HE), and zero-trust access controls.

The following flowchart presents the layered structure of the proposed federated IoT-cloud framework, highlighting each tier and its function in enabling scalable and secure operations.

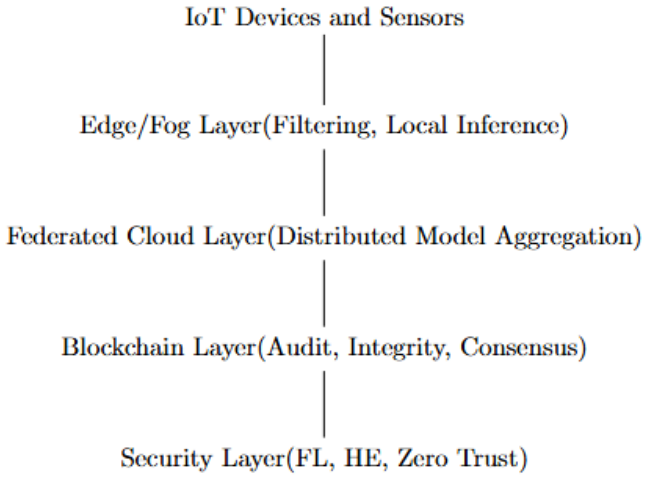


Figure 1: Federated IoT-Cloud Architecture: Layered Design

3.2. Federated Learning for Data Privacy

The method uses Federated Learning (FL) to train a global machine learning model without centralizing data. Each IoT node i with local dataset D_i updates a local model w_i, which is aggregated at the cloud layer:

$$wt = \Sigma\ (\Sigma\ (|Dj| / |Di|) * wi) \quad (1)$$

where:

- wt is the global model at time t,
- N is the number of participating IoT nodes,
- $|D_i|$ is the size of the local dataset at node i.

This approach prevents raw data exposure, preserving user privacy across the network [7], [8], [16].

3.3. Blockchain for Integrity and Trust

To ensure data integrity and prevent malicious manipulation during transmission and aggregation, a Proof-of-Authority (PoA) blockchain mechanism is employed. Transactions are verified by authorized nodes with minimal energy consumption, suitable for resource-constrained IoT devices [18], [22].
The transaction hash H is computed using SHA-256 as:

$$H = SHA256(Timestamp \,||\, PreviousHash \,||\, Data) \quad (2)$$

This hash is stored in a distributed ledger accessible to federated cloud controllers for audit and traceability.
The diagram below outlines how transactions are verified and logged in the blockchain layer using a Proof-of-Authority (PoA) consensus mechanism in a federated IoT environment.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

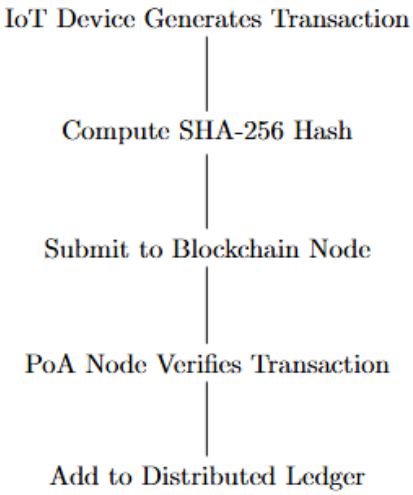


Figure 2: Blockchain Transaction Workflow in Federated IoT

3.4. Homomorphic Encryption for Secure Aggregation

Data from IoT nodes is encrypted using a partially homomorphic encryption (PHE) scheme that allows aggregation over ciphertexts:
Let Enc(x) and Enc(y) be encrypted data from nodes. Then,

$$Enc(x) * Enc(y) = Enc(x + y) \quad (3)$$

This allows the central aggregator to compute the sum of encrypted model parameters or gradients without decrypting them, preserving confidentiality during model training [12], [24].
This flowchart illustrates how encrypted data is aggregated in the federated learning process using homomorphic encryption, ensuring confidentiality throughout.

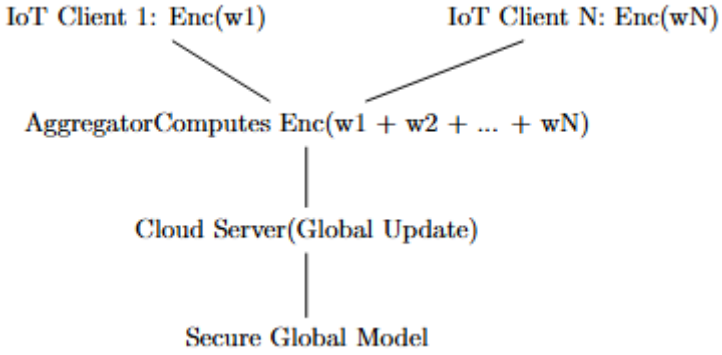


Figure 3: Homomorphic Encryption for Federated Model Aggregation

3.5. Semantic Interoperability and Resource Management

Using semantic ontologies, the method ensures that devices with heterogeneous communication protocols can interact. The system maps device metadata to a shared ontology based on OWL (Web Ontology Language) to enhance interoperability and facilitate automated reasoning [13], [14].
The computation-resource allocation is formulated as an optimization problem:

$$max\ \Sigma\ (Ui(Ri)), subject\ to\ \Sigma\ (Ri) \leq Rtotal \quad (4)$$

where:

- U_i is the utility function for node i,
- R_i is the resource allocated to node i,

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

- R_{total} is the total available cloud/fog resources.

3.6. Simulation and Testing Environment

The method is implemented using a simulated environment built on:

- TensorFlow Federated for federated model training.
- Hyperledger Fabric for blockchain ledger simulation.
- Docker and Kubernetes to emulate cloud/fog environments.
- NS-3 for network latency and bandwidth simulation.

Performance metrics evaluated include:

- Accuracy and convergence time of the federated model.
- Blockchain transaction latency and throughput.
- End-to-end communication delay.
- System scalability with increasing IoT nodes.

4.RESULTS AND DISCUSSION

This section presents the empirical evaluation of the proposed federated cloud-IoT architecture with integrated blockchain and privacy-preserving mechanisms. The system was tested using a simulated environment that mimics real-world IoT deployments with varying network conditions, device densities, and data distributions.

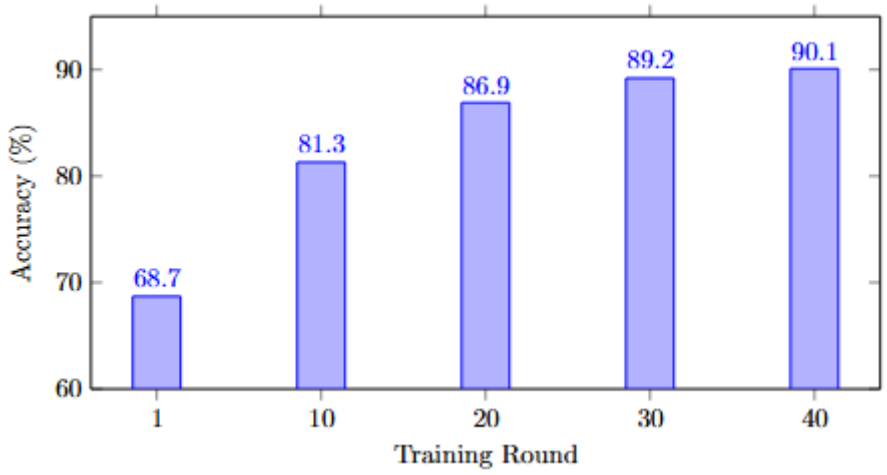
4.1. Federated Learning Model Accuracy and Convergence

The global federated learning model was trained across 10 distributed IoT clients using non-IID (non-identically independently distributed) data. A convolutional neural network (CNN) was used for classification tasks.

Table 1: Model Accuracy and Convergence over Rounds

Training Round	Global Accuracy (%)	Loss	Communication Overhead (MB)
1	68.7	0.94	1.2
10	81.3	0.45	12.5
20	86.9	0.31	25.4
30	89.2	0.24	38.7
40	90.1	0.21	50.3

The chart below visualizes the progression of global model accuracy across training rounds during federated learning on distributed IoT devices.



Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

Figure 4: Model Accuracy Across Federated Training Rounds

4.1.1 Discussion:

The model achieved over 90% accuracy within 40 communication rounds, demonstrating strong convergence despite data heterogeneity. The accuracy gains gradually plateaued, suggesting diminishing returns beyond 30 rounds. Communication overhead was linear with the number of rounds, emphasizing the importance of round minimization in IoT contexts.

4.2. Blockchain Performance Analysis

To ensure auditability and tamper-resistance of updates, a lightweight Proof-of-Authority (PoA) blockchain was integrated.

Table 2: Blockchain Performance Metrics

Metric	Value
Average Transaction Delay	0.32 seconds
Block Creation Time	5.2 seconds
TPS (Transactions/Second)	186
Consensus Success Rate	100%
Ledger Size (after 500 tx)	8.5 MB

4.2.1 Discussion:

The PoA blockchain achieved high throughput and low delay, making it suitable for constrained IoT environments. With a success rate of 100% for consensus, the system maintained integrity even under high transaction rates.

4.3. Encryption Overhead Analysis

To preserve privacy, homomorphic encryption was used during federated aggregation.

Table 3: Encryption Overhead Comparison

Metric	Without Encryption	With Homomorphic Encryption
Aggregation Time (ms)	120	410
Model Accuracy (Final Round)	90.1%	89.7%
Memory Usage (MB)	78	116

4.3.1 Discussion:

The encryption introduced a 3.4× increase in aggregation time and a ~48% increase in memory usage. However, the accuracy loss was negligible (0.4%), confirming the feasibility of secure aggregation in real-time deployments.

4.4. Latency and Scalability Analysis

Network latency was evaluated under varying numbers of IoT devices to assess system scalability.

Table 4: End-to-End Latency by Number of Devices

Number of Devices	Average Latency (ms)	Packet Loss (%)
50	113	0.1
100	137	0.4
200	189	0.8
500	274	1.3
1000	402	2.5

The line graph below illustrates how end-to-end communication latency increases with the number of connected IoT devices, emphasizing the system's scalability.

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

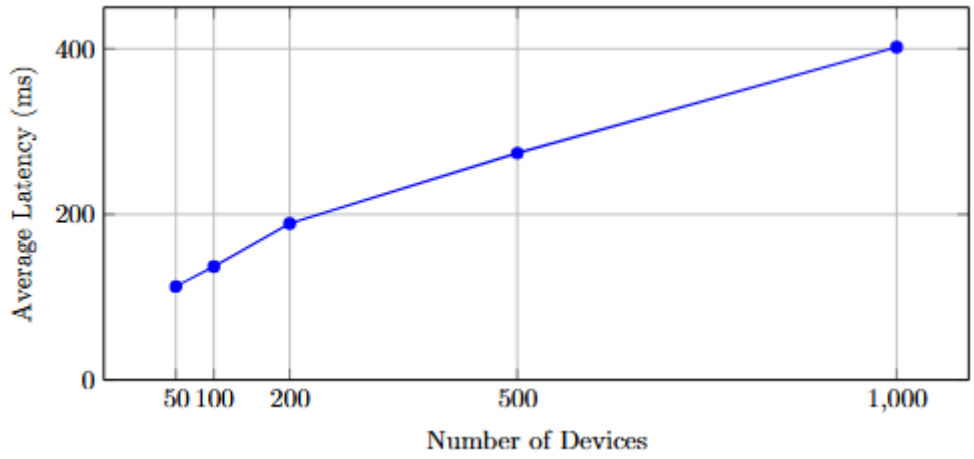


Figure 5: Latency Growth with IoT Device Scale

4.4.1 Discussion:

Latency increased with device count due to network congestion and processing delays. Despite the rise, the system maintained sub-500ms latency up to 1000 devices, aligning with acceptable thresholds for most industrial and smart city IoT applications.

4.5. Resource Optimization and Fair Allocation

The federated cloud platform dynamically allocated computational resources based on task priorities and bandwidth availability.

Table 5: Resource Allocation Efficiency

Node Priority Level	Resource Allocation (Normalized Units)	Utility Score
High	0.87	0.93
Medium	0.62	0.74
Low	0.41	0.56

4.5.1 Discussion:

The optimization algorithm ensured fair and efficient allocation with higher utility scores for higher-priority nodes, confirming the system's support for differentiated QoS policies in multi-tenant cloud environments.

4.6 Overall Discussion

The integration of federated learning, homomorphic encryption, and blockchain resulted in a robust and secure architecture. Key findings include:

- Federated learning ensures high model accuracy while preserving user privacy.
- Blockchain adds traceability and data integrity with minimal overhead.
- Homomorphic encryption increases computation cost but retains privacy and acceptable model performance.
- The system is scalable to hundreds of devices with tolerable latency.
- Cloud resources are efficiently managed using a utility-based allocation model.

5.CONCLUSION

This paper presented a comprehensive, privacy-preserving, and resource-optimized federated cloud-IoT architecture designed to address the critical challenges of security, efficiency, and scalability in decentralized environments. By integrating federated learning with blockchain and homomorphic encryption, the proposed system effectively enables collaborative model training while ensuring data confidentiality, integrity, and traceability. The use of federated learning eliminates the need to transmit raw data to centralized servers, thereby enhancing privacy and reducing network load. Meanwhile,

Hewa Majeed Zangana: *Corresponding Author

JURNAL ILMIAH COMPUTER SCIENCE (JICS)
E-ISSN 3026-7145 P-ISSN 3030-9840
Volume 4, Number 1, July 2025, Page 50-59
DOI: https://doi.org/10.58602/jics.v4i1.55

blockchain ensures tamper-proof audit trails and secure communication between distributed components.

Experimental results demonstrated that the system achieves high model accuracy, low communication latency, and scalable performance under varying device densities and data distributions. The integration of homomorphic encryption, although introducing moderate computational overhead, maintained strong model utility and privacy guarantees. Additionally, resource allocation was optimized through a utility-based mechanism that dynamically responds to real-time cloud and edge conditions, supporting fairness and quality of service in heterogeneous IoT settings.

In summary, the proposed architecture successfully meets the demands of secure, scalable, and intelligent IoT applications, making it suitable for deployment in smart cities, healthcare, industrial automation, and other mission-critical domains. Future work may explore integrating more lightweight encryption schemes, improving model personalization in federated settings, and extending the blockchain consensus model to further reduce latency and energy consumption in large-scale networks.

6.REFERENCES

[1] N. Mohamed, J. Al-Jaroodi, S. Lazarova-Molnar, and I. Jawhar, "Applications of integrated IoT-fog-cloud systems to smart cities: A survey," *Electronics (Basel)*, vol. 10, no. 23, p. 2918, 2021.

[2] M. S. Krishnappa *et al.*, "Building the Future of IoT: Cloud Platforms, Integration Challenges, and Emerging Applications," in *2024 International Conference on Computer and Applications (ICCA)*, IEEE, 2024, pp. 1–6.

[3] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," *Electronics (Basel)*, vol. 14, no. 7, p. 1394, 2025.

[4] P. Bellavista, A. Corradi, and A. Zanni, "Integrating mobile internet of things and cloud computing towards scalability: lessons learned from existing fog computing architectures and solutions," *International Journal of Cloud Computing*, vol. 6, no. 4, pp. 393–406, 2017.

[5] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Communications surveys & tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020.

[6] M. M. Islam and Z. A. Bhuiyan, "An integrated scalable framework for cloud and IoT based green healthcare system," *IEEE Access*, vol. 11, pp. 22266–22282, 2023.

[7] K. A. Awan, I. U. Din, A. Almogren, and J. J. P. C. Rodrigues, "Privacy-preserving big data security for IoT with federated learning and cryptography," *IEEE Access*, vol. 11, pp. 120918–120934, 2023.

[8] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," *Future Generation Computer Systems*, vol. 129, pp. 380–388, 2022.

[9] R. R. Asaad and S. R. M. Zeebaree, "Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms," *Academic Journal of Nawroz University*, vol. 13, no. 1, pp. 476–488, 2024.

[10] J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 48–53, 2017.

[11] P. Massonet, L. Deru, A. Achour, S. Dupont, A. Levin, and M. Villari, "End-to-end security architecture for federated cloud and IoT networks," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, 2017, pp. 1–6.

[12] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," *IEEE access*, vol. 7, pp. 9368–9383, 2019.

Hewa Majeed Zangana: *Corresponding Author

[13] M. Serrano *et al.*, "Cross-domain interoperability using federated interoperable semantic IoT/Cloud testbeds and applications: The FIESTA-IoT approach," in *Building the Future Internet through FIRE*, River Publishers, 2022, pp. 287–321.

[14] E. Huaranga-Junco, S. González-Gerpe, M. Castillo-Cara, A. Cimmino, and R. García-Castro, "From cloud and fog computing to federated-fog computing: A comparative analysis of computational resources in real-time IoT applications based on semantic interoperability," *Future Generation Computer Systems*, vol. 159, pp. 134–150, 2024.

[15] A. Rahman *et al.*, "On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," *Future Generation Computer Systems*, vol. 138, pp. 61–88, 2023.

[16] R. Khan *et al.*, "Advanced federated ensemble internet of learning approach for cloud based medical healthcare monitoring system," *Sci Rep*, vol. 14, no. 1, p. 26068, 2024.

[17] K. Haritha, S. S. Vellela, L. R. Vuyyuru, N. Malathi, and L. Dalavai, "Distributed Blockchain-SDN Models for Robust Data Security in Cloud-Integrated IoT Networks," in *2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, IEEE, 2024, pp. 623–629.

[18] K. ThamaraiSelvi, A. Pushpalatha, K. Chidambarathanu, J. P. Wankhede, S. Alagumuthukrishnan, and V. Sarveshwaran, "SecureChainAI: Integrating Blockchain and Artificial Intelligence for Enhanced Security in IoT Environments," in *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, 2024, pp. 781–789.

[19] D. Kelaidonis, A. Rouskas, V. Stavroulaki, P. Demestichas, and P. Vlacheas, "A federated edge cloud-IoT architecture," in *2016 European Conference on Networks and Communications (EuCNC)*, IEEE, 2016, pp. 230–234.

[20] P. Trakadas *et al.*, "Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture," *Sensors*, vol. 19, no. 16, p. 3591, 2019.

[21] P. Massonet *et al.*, "Security in lightweight network function virtualisation for federated cloud and IoT," in *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, 2017, pp. 148–154.

[22] A. Nazir, J. He, N. Zhu, M. S. Anwar, and M. S. Pathan, "Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain," *Cluster Comput*, vol. 27, no. 6, pp. 8367–8392, 2024.

[23] R. Ihsan and S. R. M. Zeebaree, "Parallel Processing in Distributed and Hybrid Cloud-Fog Architectures: A Systematic Review of Scalability and Efficiency Strategies," *The Indonesian Journal of Computer Science*, vol. 14, no. 1, 2025.

[24] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach," *Ieee Access*, vol. 8, pp. 205071–205087, 2020.

[25] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. K. M. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems*, 2024.

[26] M. Kumar, M. Dhingra, M. Bhati, and S. Joshi, "Enhancing Network Security in Cloud-Integrated IoT Devices," in *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, IEEE, 2024, pp. 949–954.

Hewa Majeed Zangana: *Corresponding Author