ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 10, No. 6, 65-76 (2025)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ
ISSN: 2415-6698

Federated Learning with Differential Privacy and Blockchain for Security and Privacy in IoMT

A Theoretical Comparison and Review

Shaista Ashraf Farooqi*[1], Aedah Abd Rahman[1], Amna Saad[2]

[1]*Asia e University (AeU) Wisma Subang Jaya, Jalan SS 15/4, Subang Jaya, Malaysia*

[2]*Universiti Kuala Lumpur, Malaysian Institute of Information Technology, 1016 Jalan Sultan Ismail, 50250 Kuala Lumpur, Malaysia*

Email(s): aedah.abdrahman@aeu.edu.my (A. A. Rahman), amna@unikl.edu.my (A. Saad)

*Corresponding Author: Shaista Ashraf Farooqi, Asia e University (AeU) Wisma Subang Jaya, Jalan SS 15/4, Subang Jaya, Malaysia. shaista_ashraf@yahoo.com

ARTICLE INFO

Article history:
Received: 11October, 2025
Revised: 27 November, 2025
Accepted: 29 November, 2025
Online: 15 December, 2025

Keywords:
Internet of Medical Things IoMT
Federated Learning
Differential Privacy
Blockchain
Scalability
Security and Privacy
Decentralized Systems

ABSTRACT

The growing integration of the Internet of Medical Things (IoMT) into healthcare has amplified the need for secure and privacy-preserving artificial intelligence. Federated Learning (FL) has emerged as a pivotal paradigm for decentralized medical data processing; however, it still faces challenges concerning data confidentiality, trust management, and scalability. This review presents an extended theoretical comparison of two prominent privacy-preserving frameworks—Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC)—to assess their suitability for ensuring data security, transparency, and regulatory compliance in IoMT environments. The FL-DP framework safeguards patient data through noise injection during model updates, offering mathematically proven privacy guarantees. Conversely, the FL-BC framework reinforces trust and integrity via immutable ledgers and consensus mechanisms such as Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT). Reviewing literature published between 2021 and 2025, this study examines trade-offs in privacy, scalability, latency, and energy efficiency, while highlighting emerging hybrid architectures that integrate both approaches. The findings reveal that FL-DP provides stronger privacy control, whereas FL-BC ensures verifiable trust and traceability—together forming the foundation for next-generation secure and trustworthy federated learning systems in IoMT-driven healthcare.

1. Introduction

This paper is an extended version of our earlier work, "*A Theoretical Comparison of Federated Learning with Differential Privacy and Blockchain for Security and Privacy in IoMT*," originally presented in [1] The conference paper established a foundational comparison between Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC), emphasizing their roles in improving privacy, trust, and scalability in decentralized healthcare systems.

Building upon that initial study, the present journal version provides a broader theoretical framework, a comprehensive literature review (2021–2025), and a deeper analysis of the privacy–utility–trust trade-offs, scalability, and compliance implications associated with both frameworks. Furthermore, this paper introduces an extended hybrid conceptual model integrating

DP and Blockchain for holistic privacy preservation and distributed trust management in Federated Learning environments.

The growing network of smart medical devices is reshaping healthcare globally by enabling continuous remote monitoring and intelligent diagnostics through connected medical devices. It plays a critical role in predictive medicine by facilitating earlier disease detection, personalized treatments, and improved clinical outcomes. Wearable sensors and embedded devices continuously track vital signs, enabling healthcare providers to make real-time, data-driven interventions.

Additionally, IoMT promotes remote healthcare delivery for patients in underserved or rural areas, reducing hospitalization

https://dx.doi.org/10.25046/aj100606

rates and enhancing access to medical services. According to recent industry projections, the IoMT market size is anticipated to reach USD 188 billion by 2028, highlighting the growing interconnection between clinical systems and intelligent medical devices [2].

Despite its revolutionary potential, IoMT's distributed nature exposes it to severe privacy, security, and scalability challenges. Sensitive patient information traversing heterogeneous networks can be intercepted, manipulated, or exploited, resulting in data breaches and cyberattacks.

In addition, the US Health Insurance Portability and Accountability Act (HIPAA) and the European Union General Data Protection Regulation (EU GDPR) pose significant compliance challenges, particularly concerning the storage, processing, and sharing of healthcare data [3] These challenges underscore the need for advanced, privacy-preserving computational paradigms that can analyze distributed data without compromising confidentiality.

In modern healthcare systems, collaboration across hospitals, laboratories, and wearable devices has become essential for building intelligent models. Through the use of federated learning, these entities can jointly train a shared global model without transferring raw data. This approach keeps sensitive information local, ensuring both data privacy and patient confidentiality [4]. Although federated learning reduces the risks that come with centralized data storage, it also introduces new security challenges. Among these are inference attacks, data poisoning, and model inversion threats. Such attacks may reveal sensitive data hidden in the model updates shared between clients and the server.

To address these limitations, researchers have proposed two major enhancement frameworks:

i. *Federated Learning with Differential Privacy (FL-DP),* which injects mathematically calibrated noise into model gradients or parameters to ensure formal privacy guarantees (ε, δ); and
ii. *Federated Learning with Blockchain (FL-BC),* which leverages distributed consensus, immutability, and cryptographic integrity to eliminate single points of failure and enhance trust among participants [5], [6].

While both frameworks contribute toward improving privacy and security, they differ fundamentally in design, scope, and scalability. FL-DP emphasizes data confidentiality through controlled noise and privacy budgets, whereas FL-BC ensures system integrity and auditability through decentralized verification mechanisms. The selection of one framework over the other depends on application-specific requirements such as latency, computational resources, trust models, and compliance obligations.

This extended paper systematically reviews, compares, and synthesizes these two approaches, presenting a multi-dimensional theoretical analysis that spans privacy guarantees, trust mechanisms, computational efficiency, scalability, and compliance readiness. The main objectives of this extended version are to:

i. Provide a comprehensive review (2021–2025) of existing FL-DP and FL-Blockchain research;
ii. Theoretically evaluate their security, privacy, and scalability trade-offs in distributed learning;
iii. Propose an integrated hybrid architecture that unifies DP's formal privacy mechanisms with Blockchain's decentralized trust model; and
iv. Identify open challenges and research directions for future federated systems in data-sensitive domains.

The subsequent sections are arranged in the following manner. Section II presents a detailed review of literature, summarizing key advances in FL-DP and FL-Blockchain frameworks. Section III outlines the theoretical foundations and comparative analysis model. Section IV discusses hybrid integration opportunities and open research challenges. Section V concludes with future perspectives on developing scalable, compliant, and privacy-preserving federated learning ecosystems.

2. Related Work

The advancement of connected medical technologies has given rise to the Internet of Medical Things (IoMT)—a network of interconnected healthcare devices that continuously collect, transmit, and analyze patient data in real time. This paradigm shift has accelerated innovations in personalized healthcare, remote monitoring, and predictive diagnostics, yet it has also introduced serious challenges in data privacy, system security, and computational scalability [7] The sensitive nature of medical data and the distributed operation of IoMT systems make them particularly vulnerable to data breaches, model poisoning, and inference attacks, prompting extensive research into privacy-preserving and trustworthy machine learning frameworks [8]-[9].

Recent studies have emphasized the need for decentralized learning models that eliminate the reliance on centralized data repositories. To address these issues, federated learning (FL) offers a promising way for multiple participants, such as hospitals, laboratories, and wearable devices—to collaboratively train models while retaining data locally.

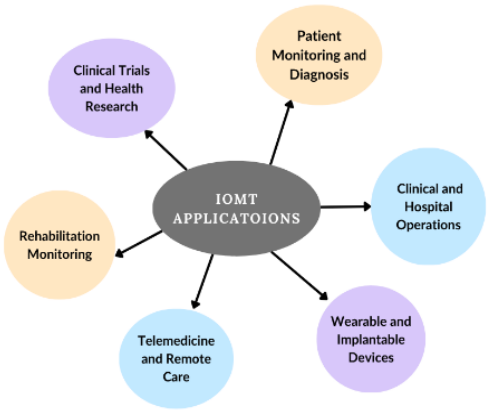

Figure 1: Various IoMT Applications

However, despite its potential to enhance privacy and scalability, FL remains vulnerable to gradient leakage, adversarial updates, and trust issues among participating entities [10]-[11]. To address these gaps, advanced frameworks combining Differential Privacy (DP) and Blockchain have been proposed, offering

complementary protection mechanisms for secure collaborative learning.

Figure 1 provides an overview of key applications of the Internet of Medical Things (IoMT) across modern healthcare systems.

2.1. Federated Learning (FL)

Federated Learning decentralizes the conventional machine-learning pipeline by allowing multiple clients—such as hospitals, laboratories, or edge gateways—to train local models on private datasets while sharing only encrypted or aggregated parameter updates with a central coordinator [12]. The classical workflow relies on periodic communication rounds in which each participant performs local training, transmits model gradients or weights, and receives the globally aggregated model computed through algorithms such as Federated Averaging (FedAvg) [13].

Although FL mitigates direct data exposure, several vulnerabilities remain. Gradient leakage and model inversion attacks can reconstruct sensitive features from transmitted updates, whereas data poisoning and backdoor manipulation threaten model integrity [14], [15]. Furthermore, heterogeneity in data distribution (non-IID conditions), computational power, and network bandwidth across IoMT devices leads to bias and instability in global convergence [16]. Communication inefficiency is another constraint; frequent synchronization between hundreds of clients increases latency and energy consumption, especially in bandwidth-limited healthcare networks [17]. To alleviate these issues, research trends emphasize secure aggregation protocols, adaptive client participation, and compression-based communication schemes, yet the fundamental trust and confidentiality gap persists—motivating the incorporation of additional cryptographic and decentralized components.

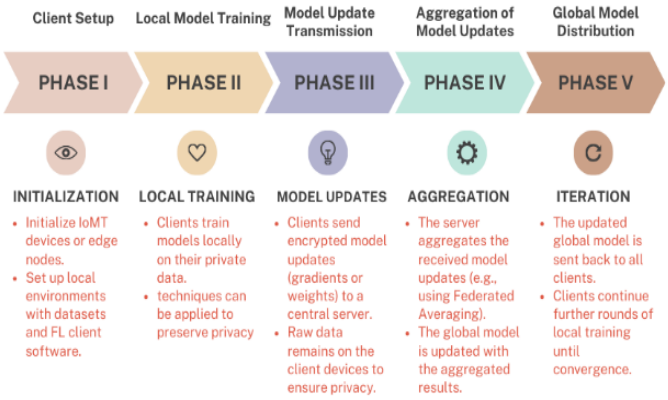

Figure 2. Phases of the Federated Learning process

Adding Differential Privacy (DP) to the FL framework by injecting controlled noise into model updates protects the anonymity of individual data contributions. The architecture must consider the differences among client devices, which vary in computational power, network bandwidth, and data types, leading to non-IID data and potential delays. Reducing communication overhead is vital for large-scale FL systems in bandwidth-limited IoMT environments, requiring optimized protocols and protection against attacks through methods like Byzantine fault tolerance and possible blockchain integration [18]. Figure 2. illustrates the different phases of the Federated Learning process, from local model training to global aggregation and model redistribution.

2.2. Integration of Differential Privacy within Federated Learning

Differential Privacy (DP) protects sensitive information by injecting carefully calibrated statistical noise into model calculations. A randomized mechanism M satisfies (ε, δ)-DP if for any neighboring datasets D and D′, differing by one record, and for any possible output S,

$$\Pr [M(D) \in S] \leq e \, \varepsilon \Pr [M(D') \in S] + \delta \quad (1)$$

where ε quantifies the privacy loss and δ bounds the probability of exceeding it [18]. In FL, DP can be applied either locally—each client perturbs its updates before transmission—or globally—noise is added by the aggregator. The local variant offers stronger confidentiality but degrades accuracy more severely.

Between 2021 and 2025, research has focused on optimizing the privacy–utility balance by adaptive noise scheduling, gradient clipping, and sensitivity-based budget allocation [19]. Some works employ input-discriminative local DP to allocate smaller budgets to less-sensitive features and larger budgets to high-risk attributes [20]. Others combine DP with Secure Multi-Party Computation (SMPC) or Homomorphic Encryption (HE) to protect updates during aggregation [21], [22]. Despite these advances, practical deployment faces obstacles:

i. Excessive noise in high-dimensional medical datasets diminishes diagnostic accuracy;
ii. Cumulative privacy loss across multiple rounds complicates budget management; and
iii. Resource-constrained IoMT nodes struggle to perform the additional arithmetic required for DP perturbation.

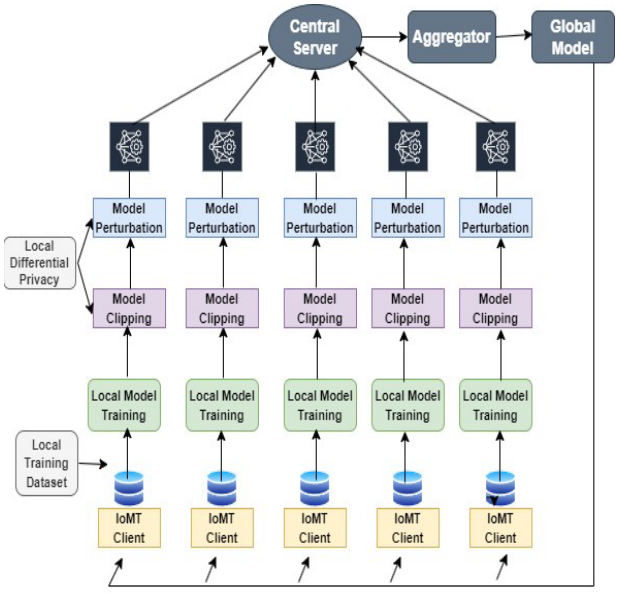

Figure 3. Federated Learning with Differential Privacy (FL-DP) framework

Consequently, while DP provides mathematical confidentiality guarantees, it lacks mechanisms for auditability and distributed consensus, making it complementary—but not sufficient—for

end-to-end trust establishment. Figure 3 presents the architectural design of the Federated Learning with Differential Privacy (FL-DP) framework, demonstrating how client-level noise addition and secure aggregation jointly ensure data confidentiality and model utility.

2.3. Blockchain for Secure Federated Learning

Blockchain technology introduces decentralization, transparency, and immutability into collaborative learning environments [23]. By storing each model update as a cryptographically linked transaction, Blockchain eliminates reliance on a single central server and enables tamper-proof logging. Consensus algorithms such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), and BFT (Byzantine Fault Tolerance) validate contributions and ensure ledger consistency [24].

Applied to FL, Blockchain offers multiple security benefits:

i. Integrity Assurance —each update is verifiable and immutable;
ii. Trust Establishment —participants can confirm authenticity without a central authority;
iii. Traceability and Accountability —complete histories of model contributions are maintained; and
iv. Resilience to Single-Point Failures —distributed validation enhances fault tolerance.

Empirical studies have demonstrated that blockchain-enhanced FL architectures can detect tampering and improve reliability in distributed healthcare and industrial networks [25], [26], [27], [28]. However, these benefits are accompanied by significant trade-offs. Consensus formation increases computational cost, latency, and energy demand, which are particularly problematic for lightweight edge or IoMT devices. Moreover, the immutability of Blockchain conflicts with regulatory requirements such as the GDPR Articles 16 and 17 ("right to rectification and erasure"), necessitating auxiliary designs like off-chain storage or ZKPs (zero-knowledge proofs) [29]. Therefore, while Blockchain strengthens integrity and transparency, its direct adoption in real-time federated environments remains constrained by scalability and compliance limitations. Figure 4 provides an overview of the Federated Learning framework integrated with Blockchain technology.

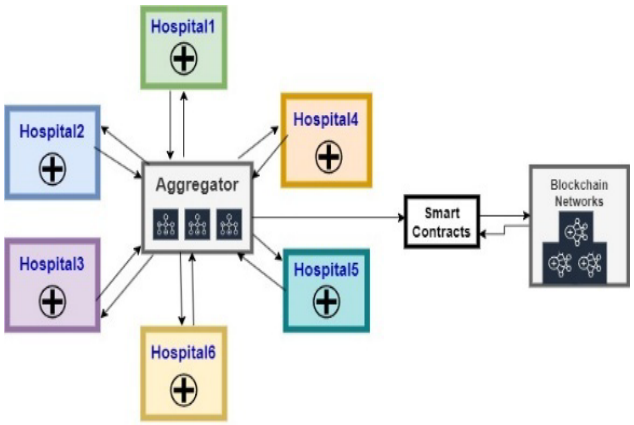

Figure 4. Federated Learning with Blockchain Framework

2.4. Comparative and Hybrid Frameworks

To overcome the individual shortcomings of DP and Blockchain, recent research trends favor hybrid frameworks that exploit their complementary strengths [30], [31], [32]. In these designs, DP provides quantifiable privacy protection at the data or gradient level, whereas Blockchain ensures global trust and tamper resistance at the system level. Model updates are first sanitized through DP mechanisms and then validated and recorded on a Blockchain ledger, establishing dual-layer protection. Such integration enhances resilience against both inference attacks and malicious parameter manipulation.

Nevertheless, existing hybrid approaches often emphasize prototype implementation rather than rigorous theoretical evaluation. Comprehensive comparisons that analyze privacy-utility trade-offs, energy consumption, latency, and regulatory compliance across the two paradigms remain limited. In particular, few studies address how privacy budgets (ε, δ) interact with consensus latency and block-generation frequency—an essential consideration for time-critical medical applications.

2.5. Summary of Research Gaps

The state of the art reveals three persistent deficiencies:

i. Absence of integrated theoretical models that holistically compare FL-DP and FL-Blockchain across multidimensional evaluation metrics including privacy strength, scalability, communication overhead, and compliance readiness.
ii. Limited discussion of governance and regulation, particularly the reconciliation of formal privacy frameworks with legal standards such as HIPAA and GDPR within decentralized architectures.
iii. Inadequate hybridization strategies capable of simultaneously delivering strong privacy guarantees, verifiable trust, and real-time efficiency for heterogeneous IoMT and edge-intelligence ecosystems.

The present paper addresses these gaps by conducting a comprehensive theoretical comparison and a synthesized review of contemporary developments (2021–2025). It further introduces a hybrid conceptual architecture that combines Differential Privacy's mathematical confidentiality with Blockchain's decentralized trust management to create secure, transparent, and regulation-compliant federated learning systems.

3. Theoretical Framework and Comparative Analysis

The integration of Differential Privacy (DP) and Blockchain into Federated Learning (FL) creates two distinct but conceptually overlapping frameworks for secure, privacy-preserving distributed intelligence. Both frameworks address critical vulnerabilities of conventional FL but differ in their underlying security models, communication architecture, and computational dynamics. This section presents the theoretical basis of each framework, followed by a multi-dimensional comparison across key metrics such as privacy strength, trust assurance, scalability, latency, and compliance readiness.

3.1. Federated Learning Framework

In a typical Federated Learning system [33], a set of N clients $\{C_1, C_2, \dots, C_N\}$ collaboratively train a global model w coordinated by a central aggregator. Each client C_i holds a local dataset D_i and updates the model parameters using gradient descent. The local objective function is:

$$F_i(w) = \frac{1}{|D_i|}\sum_{x_j \in D_i} \mathcal{L}(w; x_j) \quad (2)$$

where $\mathcal{L}(\cdot)$ is the loss function.

The global objective across all clients is minimized as:

$$F(w) = \sum_{i=1}^{N} \frac{|D_i|}{|D|} F_i(w) \quad (3)$$

During each communication round t, local clients compute updates:

$$w_i^{t+1} = w^t - \eta \nabla F_i(w^t) \quad (4)$$

where η is the learning rate. The server aggregates these updates via Federated Averaging (FedAvg):

$$w^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{t+1} \quad (5)$$

While this aggregation preserves data locality, it does not inherently prevent gradient leakage or ensure integrity of updates. To mitigate these risks, privacy and security enhancements through DP and Blockchain have been proposed.

3.2. Differential Privacy-Enhanced Federated Learning (FL-DP)

The FL-DP framework strengthens client privacy by applying differential privacy during gradient transmission or aggregation. The formal definition of (ε, δ)-Differential Privacy [34] ensures that the inclusion or exclusion of any data point minimally affects the model output:

$$\Pr[\mathrm{M}(\mathrm{D}) \in \mathrm{S}] \leq \mathrm{E}^{\mathrm{E}} \Pr[\mathrm{M}(\mathrm{D}') \in \mathrm{S}] + \Delta \quad (6)$$

where D and D' differ by one record, M is the randomized mechanism, and S is the subset of possible outputs.

In FL-DP, local updates are first clipped to a predefined sensitivity bound C to control gradient magnitude:

$$\tilde{g}_i = \frac{g_i}{\max\left(1, \frac{\|g_i\|_2}{C}\right)} \quad (7)$$

and Gaussian noise $\mathcal{N}(0, \sigma^2 \mathrm{C}^2)$ is added before aggregation:

$$\hat{\mathrm{g}}_\mathrm{i} = \tilde{\mathrm{g}}_\mathrm{i} + \mathcal{N}(0, \sigma^2 \mathrm{C}^2) \quad (8)$$

The privacy budget ε defines the trade-off between privacy and accuracy — smaller ε yields higher privacy but introduces more noise, reducing model utility [35].

The cumulative privacy loss after T rounds is bounded using composition theorems:

$$\varepsilon_{total} \leq \sqrt{2T \ln(1/\delta)} \cdot \varepsilon + T\varepsilon(e^{\varepsilon} - 1) \quad (9)$$

Advantages of FL-DP

i. Formal mathematical guarantees of individual data protection.
ii. Compatibility with GDPR and HIPAA standards.
iii. Lightweight computational cost suitable for IoMT and edge devices.

Limitations

i. Gradual degradation of model accuracy with increasing noise.
ii. Privacy budget exhaustion over multiple communication rounds.
iii. Centralized aggregator remains a potential single point of trust failure.

In summary, Differential Privacy fortifies Federated Learning with formal, quantifiable confidentiality guarantees, enabling secure model updates without direct data exposure; however, its reliance on centralized aggregation and sensitivity to noise-induced utility loss necessitate complementary mechanisms—such as Blockchain—to achieve end-to-end trust and integrity in decentralized learning environments.

3.3. Blockchain-Integrated Federated Learning (FL-BC)

The FL-Blockchain framework decentralizes model aggregation by recording each client's model update on a distributed ledger. Rather than relying on a single trusted server, participating nodes validate and reach consensus on the authenticity of model updates before integration [36].

Each local model update w_i^t is converted into a transaction T_i^t and broadcast to the network. The transaction includes:

$$T_i^t = (ID_i, h(w_i^t), Sig_i, Time_t) \quad (10)$$

where $h(\cdot)$ is the hash function ensuring immutability and Sig_i is the client's digital signature.

Blocks B_k consist of validated transactions $\{T_i^t\}$ and are chained via cryptographic hashes:

$$B_k = \{T_i^t, h(B_{k-1}), Time_k, Sign_{miner}\} \quad (11)$$

Consensus protocols such as Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT) determine the validity of each block. The expected consensus delay D_c is approximately proportional to the number of participating nodes N and the time per validation τ_v:

$$D_c \propto N \times \tau_v \quad (12)$$

This relationship indicates that as the number of participating nodes or the validation time increases, the overall consensus latency rises proportionally, highlighting the scalability-performance trade-off inherent in blockchain-based federated learning systems [37].

Advantages of FL-Blockchain

i. Decentralized trust model eliminates the single point of failure.
ii. Immutable and auditable transaction history ensures data integrity.
iii. Enables traceability and accountability across federated participants.

Limitations

i. High computational and communication overhead due to consensus.
ii. Energy consumption unsuitable for resource-limited IoMT devices.
iii. Immutability complicates GDPR compliance ("right to erasure").

In conclusion, Blockchain integration enhances Federated Learning by introducing decentralized consensus, immutable record-keeping, and verifiable trust among participants; however, its computational complexity, energy cost, and potential regulatory conflicts underscore the need for hybrid designs that combine Blockchain's integrity assurance with Differential Privacy's formal confidentiality guarantees.

3.4. Layered Architectural Analysis

Since Differential Privacy and Blockchain operate through very different mechanisms within the Federated Learning ecosystem, it is important to analyze how each one contributes to overall system security and efficiency. FL-DP focuses on protecting data confidentiality by adding controlled noise and managing privacy budgets [38], whereas FL-BC ensures decentralized trust and data integrity through consensus validation and immutable ledgers [39]. This analysis examines both frameworks across three key dimensions — the data layer, model layer, and trust layer — to highlight their strengths, limitations, and potential integration points in building a unified privacy-preserving federated learning architecture. Table 1 provides a comparative representation of FL-DP and FL-BC across three key operational layers.

Table 1. Three-layer comparison of FL-DP and FL-BC frameworks

Layer	FL with Differential Privacy (FL-DP)	FL with Blockchain (FL-BC)
Data Layer	Raw data remains localized; Gaussian or Laplace noise is injected into model updates to prevent re-identification.	Raw data remains local; encrypted model updates are converted into transactions recorded on-chain.
Model Layer	Centralized aggregation of noisy gradients using FedAvg; privacy controlled by (ε, δ).	Decentralized aggregation via consensus mechanisms (PoS, BFT); verified by all nodes.
Trust Layer	Relies on trusted central server for update aggregation; vulnerable to insider threats.	Establishes distributed trust through immutable ledgers; resistant to tampering or forgery.

The layered architectural analysis provides a structured view of how Differential Privacy and Blockchain strengthen different components of the Federated Learning pipeline. While the data layer focuses on protecting sensitive information, the model layer ensures collaborative training, and the trust layer governs transparency and accountability. Understanding the distinct functions of each layer helps identify both overlaps and gaps between the two frameworks. Building on this structural perspective, the next section presents a comparative theoretical analysis that quantitatively and qualitatively evaluates FL-DP and FL-BC across multiple performance dimensions, including privacy strength, scalability, communication cost, energy efficiency, and regulatory compliance.

3.5. Comparative Theoretical Analysis

To evaluate the relative merits of Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC), this subsection presents a systematic theoretical comparison across multiple performance dimensions—including privacy assurance, trust management, scalability, communication efficiency, energy utilization, and regulatory compliance. The analysis integrates mathematical formulations, architectural characteristics, and operational trade-offs to establish a comprehensive understanding of how each framework contributes to secure a privacy-preserving decentralized learning. Table 2 outlines the evaluation criteria employed to distinguish FL-DP from FL-BC across core operational aspects.

Table 2. Comparison criteria between FL-DP and FL-BC

Criterion	Federated Learning with Differential Privacy (FL-DP)	Federated Learning with Blockchain (FL-BC)
Privacy Mechanism	ε-DP with Gaussian or Laplace noise injection; controls exposure through noise scaling.	Cryptographic hashing, digital signatures, and distributed consensus ensure immutability.
Trust Model	Centralized; requires trust in the aggregation server.	Fully decentralized; trust distributed among nodes.
Data Integrity	Protected by central server; vulnerable to tampering if compromised.	Immutable record of updates across all participants.
Scalability	High; lightweight computation, minimal bandwidth requirement.	Limited by consensus latency and block size.
Energy Efficiency	Suitable for IoMT and edge devices.	High energy cost due to validation and block mining.

Compliance	Fully aligned with GDPR and HIPAA through formal privacy guarantees.	Conflicts with GDPR erasure rules; mitigated by off-chain storage.
Latency	Low; depends on communication rounds and privacy noise.	High; determined by consensus time and network delay.
Use Case Suitability	Privacy-critical domains (e.g., personalized healthcare, finance).	Multi-party collaborations requiring verifiable audit trails.

The comparative results highlight that each framework addresses distinct yet complementary aspects of federated system security. FL-DP excels in safeguarding individual-level data through mathematically verifiable privacy guarantees and lightweight implementation, making it ideal for latency-sensitive and resource-limited environments [40]. FL-BC, in contrast, strengthens system-level integrity and accountability through decentralized consensus and immutable audit trails, effectively mitigating insider threats and tampering risks. However, its computational overhead and regulatory challenges limit its scalability in high-frequency or energy-constrained networks [41]. Collectively, these observations suggest that neither framework alone provides a complete solution for secure federated intelligence. Instead, their integration into a hybrid FL–DP–Blockchain architecture can yield a balanced trade-off between privacy, trust, and operational efficiency—laying the foundation for the comprehensive discussion presented in the following section.

4. Discussion

The theoretical comparison of Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC) frameworks reveals two complementary paradigms, addressing privacy, security, and trust in decentralized machine learning environments. Both frameworks aim to overcome the limitations of conventional centralized training, yet their core operational principles and design objectives differ fundamentally. This section critically discusses their comparative strengths and weaknesses, practical implications, and the prospects of hybrid integration for building trustworthy, scalable federated ecosystems.

4.1. Privacy Protection and Data Confidentiality

The foremost objective of FL-DP is to ensure formal and quantifiable privacy. By injecting calibrated Gaussian or Laplacian noise into gradients, FL-DP guarantees that individual data records remain indistinguishable, even if an adversary has auxiliary information. This mathematical assurance, expressed through the privacy budget (ε, δ), provides a clear theoretical foundation for privacy measurement [42].

However, the noise-utility dilemma persists. Excessive noise reduces model accuracy and can slow convergence, especially in high-dimensional healthcare datasets. Furthermore, managing cumulative privacy loss across multiple communication rounds requires privacy accountants and budget rescaling mechanisms to avoid privacy exhaustion. Despite these limitations, FL-DP aligns naturally with data protection laws such as GDPR and HIPAA, as it inherently supports the "data minimization" and "privacy by design" principles.

In contrast, FL-Blockchain protects privacy indirectly. It ensures transaction-level confidentiality through cryptographic techniques such as hashing, encryption, and zero-knowledge proofs, but it does not conceal the metadata of transactions [43]. Hence, while Blockchain prevents tampering and falsification, it may inadvertently expose usage patterns, communication frequencies, or timestamps. Thus, Blockchain emphasizes system-level trust and transparency, whereas DP provides individual-level privacy guarantees. Both mechanisms are therefore orthogonal yet complementary—one safeguards the "what" (data), the other secures the "how" (process).

4.2. Security, Integrity, and Trust Mechanisms

Security in FL extends beyond data confidentiality—it encompasses model integrity, authentication, and auditability. In FL-DP, security primarily depends on the central server's ability to enforce privacy budgets and resist aggregation-level attacks. The introduction of secure multi-party computation (SMPC) or homomorphic encryption (HE) can mitigate these threats but increases computational overhead. Moreover, the centralized trust model still presents a single point of vulnerability; if the aggregator is compromised, all participating clients may be exposed [44].

FL-Blockchain, in contrast, transforms this trust paradigm by decentralizing authority. Consensus mechanisms such as Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT) collectively validate model updates, eliminating the need for a trusted intermediary. Each transaction is cryptographically signed, time-stamped, and permanently recorded, making it tamper-evident and auditable [45]. The immutable nature of Blockchain also prevents rollback or version manipulation attacks.

However, this decentralized robustness comes at a cost. Consensus protocols significantly increase latency, energy consumption, and communication complexity, particularly when scaling to hundreds of participating nodes. Moreover, the immutable ledger conflicts with the "right to be forgotten" stipulated in GDPR, necessitating hybrid off-chain or privacy-enhancing designs to maintain legal compliance.

Therefore, while FL-DP ensures controlled privacy leakage, FL-Blockchain guarantees trustless collaboration and tamper-proof data integrity—two distinct security frontiers essential for distributed intelligence [46].

4.3. Scalability and Communication Efficiency

Scalability remains a crucial determinant of framework suitability for real-world deployment. FL-DP exhibits comparatively high scalability because the differential noise addition is a lightweight operation, introducing minimal communication overhead. Clients transmit only perturbed gradients, and the central server performs a simple aggregation

step. This efficiency makes FL-DP ideal for IoMT, mobile edge computing, and low-power environments [46].

Conversely, FL-Blockchain's performance degrades as network size increases. Every new model update must be validated by multiple peers, serialized into a block, and propagated through the network.

The consensus delay ($D_c \propto N \times \tau_v$) grows linearly with the number of validators, making it unsuitable for time-critical applications such as emergency monitoring or remote surgery. Proposed optimizations, such as sharding, Layer-2 scaling, and side-chain protocols, alleviate some overhead but add architectural complexity [47].

Hybrid approaches that apply Blockchain selectively—for example, logging only final global updates or model checkpoints—can balance transparency with speed. Additionally, asynchronous aggregation combined with DP-based local privacy can further enhance throughput while maintaining compliance and verifiability.

4.4. Latency, Energy Consumption, and Real-Time Responsiveness

Latency and energy efficiency directly affect the feasibility of FL frameworks in large-scale medical or industrial networks. FL-DP offers lower latency because its operations primarily involve local computation and simple message passing. The most time-consuming process—noise addition—is independent of the number of participating clients. As a result, FL-DP supports real-time applications, such as continuous glucose monitoring or anomaly detection in wearable devices [48].

In contrast, Blockchain's consensus formation introduces significant latency. For example, Proof of Work (PoW)–based networks suffer from mining delays, while PoS and BFT require multiple rounds of communication to reach agreement [49]. This delay not only affects responsiveness but also increases energy consumption, rendering FL-BC less suitable for low-power IoT nodes. Alternative lightweight consensus mechanisms—Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT)—offer faster confirmation times but may reduce decentralization. Therefore, energy-aware hybrid configurations, where Blockchain operations are delegated to edge gateways or cloud nodes, present a viable compromise.

4.5. Compliance, Auditability, and Governance

Regulatory compliance has become a defining constraint in the deployment of data-driven systems, especially in healthcare and finance. FL-DP aligns naturally with legal frameworks such as HIPAA and GDPR, since differential privacy explicitly prevents re-identification and enables formal privacy accounting. Each operation can be logged and audited using the privacy budget ε, creating a verifiable record of information exposure [50].

FL-Blockchain introduces auditability by design through immutable records. Every model update and transaction is permanently logged, supporting forensic investigation and operational transparency. However, this same immutability challenges compliance with data-subject rights under GDPR Articles 16 and 17. Researchers have proposed using off-chain storage, zero-knowledge proofs (ZKPs), and private or permissioned blockchains to reconcile these conflicts. While these solutions improve compliance, they reduce decentralization, underscoring the trade-off between privacy flexibility and trust transparency [51].

4.6. Hybrid Integration: Toward Unified Privacy and Trust

The limitations of individual frameworks have motivated the emergence of hybrid FL–DP–Blockchain architectures. Such designs seek to achieve dual-layer protection by combining DP's statistical privacy with Blockchain's decentralized auditability.

In a hybrid configuration, each client first applies local differential privacy to sanitize its gradient update. The perturbed model is then encrypted and broadcast as a Blockchain transaction. Consensus nodes validate updates before inclusion in a block, ensuring authenticity and eliminating malicious contributions. Once a sufficient number of updates are validated, the aggregated model is globally updated and redistributed [52], [53], [54].

This integration produces several advantages:

- Formal privacy guarantees at the client level.
- Tamper-proof audit trails across the learning network.
- Elimination of centralized trust dependencies.
- Improved accountability and traceability for compliance audits.

However, hybridization introduces new design challenges. The combination of DP noise, encryption, and consensus overhead can increase computation and communication complexity. Effective deployment thus requires adaptive privacy budgeting, energy-efficient consensus algorithms, and off-chain storage mechanisms to maintain scalability.

4.7. Practical Implications and Domain Suitability

The findings indicate that FL-DP is most effective for privacy-sensitive and latency-critical applications such as personalized healthcare, finance, and telemedicine, where accuracy and confidentiality must coexist [55]. FL-Blockchain, on the other hand, is best suited for multi-institutional collaboration, auditable research, and public data registries, where transparency and tamper resistance outweigh real-time constraints [56].

Hybrid FL–DP–Blockchain models show potential for national health data exchanges, clinical trial collaboration, and inter-hospital machine learning initiatives, where both privacy and decentralized governance are required. By integrating lightweight Blockchain consensus with dynamic DP noise allocation, such systems could deliver trustworthy AI at scale.

4.8. Challenges and Open Research Directions

Despite the significant advancements achieved through Federated Learning with Differential Privacy (FL-DP) and Blockchain-based Federated Learning (FL-BC) frameworks, several unresolved challenges continue to hinder their large-scale adoption in IoMT environments. These open issues highlight the need for further research and technological innovation in the following areas:

i. *Dynamic Privacy Accounting:* Ensuring real-time recalibration of privacy budgets remains a major challenge. As model updates occur across multiple communication rounds, maintaining differential privacy guarantees without causing excessive accuracy loss requires adaptive noise calibration and continuous privacy tracking mechanisms.

ii. *Lightweight Consensus Protocols:* Blockchain integration in IoMT introduces high computational and energy demands. Developing lightweight, energy-efficient consensus mechanisms—optimized for edge and resource-constrained medical devices—is essential to sustain scalability and reduce latency while preserving network integrity.

iii. *Cross-Regulatory Compliance:* Global healthcare systems operate under diverse privacy regulations such as GDPR, HIPAA, and PDPA. Achieving seamless compliance within immutable blockchain frameworks demands interoperable policy layers capable of translating regulatory requirements into auditable smart contracts and metadata governance models.

iv. *Scalable Hybrid Architectures:* Designing scalable hybrid architectures is challenging because FL workflows must integrate with blockchain layers while handling high-volume, distributed healthcare data. Balancing efficient off-chain training with on-chain verification, and ensuring seamless scaling and interoperability across hospitals, edge devices, and cloud systems, adds significant complexity.

v. *Benchmarking and Standardization:* The absence of unified benchmarks and evaluation standards limits cross-framework comparison. Establishing standardized metrics for privacy loss, trust evaluation, latency, and energy consumption would enable consistent assessment and accelerate adoption in real-world healthcare systems.

Addressing these gaps will determine the feasibility of integrating FL-DP and FL-Blockchain into mainstream AI infrastructure for healthcare and other critical domains.

4.9. Summary

The discussion highlights that Federated Learning with Differential Privacy ensures mathematical privacy but lacks distributed verifiability, whereas Federated Learning with Blockchain provides trust and transparency at the expense of scalability and compliance flexibility. Integrating both paradigms within a hybrid FL–DP–Blockchain framework can reconcile these tensions by uniting formal privacy guarantees with distributed trust assurance. Such convergence represents a promising direction for developing next-generation, privacy-preserving, and regulation-aware federated learning architectures capable of powering secure, intelligent systems across diverse application domains.

5. Conclusion and Future Scope

The extended analysis, presented in this paper, provides a comprehensive theoretical comparison of two leading paradigms for secure and privacy-preserving federated learning — Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC). Both frameworks were evaluated across multiple dimensions including privacy protection, data integrity, scalability, latency, energy efficiency, and regulatory compliance. The findings reveal that while each approach contributes significantly to the security of decentralized learning, their design philosophies and operational priorities differ.

FL-DP offers formal mathematical privacy guarantees through the addition of calibrated noise, ensuring that sensitive individual information cannot be reconstructed or inferred. Its lightweight computational footprint and alignment with GDPR and HIPAA make it highly suitable for latency-sensitive and privacy-critical domains such as personalized healthcare, financial analytics, and mobile edge computing. However, the effectiveness of FL-DP is bounded by the privacy-utility trade-off and the cumulative privacy loss that arises over multiple training rounds.

In contrast, FL-Blockchain emphasizes distributed trust, transparency, and immutability. By replacing centralized aggregation with decentralized consensus, it ensures auditability and tamper resistance across all model updates. Nevertheless, high energy consumption, communication overhead, and conflicts with "right-to-erasure" provisions in regulatory frameworks restrict its scalability and practical deployment in resource-constrained environments.

The comparative synthesis suggests that these two paradigms are complementary rather than competitive. A hybrid FL–DP–Blockchain architecture can unite the statistical rigor of differential privacy with the decentralized trust of blockchain, producing an adaptive, end-to-end secure learning environment. Such integration would enable privacy-preserving model training with verifiable integrity, transparent accountability, and auditable compliance.

5.1. Research Contributions

This extended work makes the following key contributions:

i. Presents a comprehensive theoretical framework unifying privacy, trust, and scalability analysis of FL-DP and FL-BC.
ii. Expands the literature coverage (2021–2025) with systematic evaluation of privacy, communication, and compliance dimensions.
iii. Proposes a layered comparative model (data, model, and trust layers) outlining where DP and Blockchain differ or intersect in the FL ecosystem.
iv. Introduces the conceptual foundation for a hybrid FL–DP–Blockchain architecture, emphasizing privacy-trust co-optimization and regulatory conformity

5.2. Future Research Directions

While the comparative analysis highlights the promising potential of both Federated Learning with Differential Privacy (FL-DP) and Federated Learning with Blockchain (FL-BC) frameworks, several research gaps remain before these paradigms can achieve widespread, real-world implementation in IoMT-driven systems. The following directions outline potential pathways for future exploration:

i. Adaptive Privacy Budgeting

Future research should focus on developing dynamic differential privacy mechanisms that can intelligently adjust the noise scale based on model convergence rates, data sensitivity, and contextual risk factors. Such adaptive strategies would enable a more optimal balance between privacy preservation and model accuracy during iterative training.

ii. Energy-Efficient Consensus Mechanisms

Current blockchain-based consensus algorithms often incur significant energy and latency costs, making them unsuitable for IoMT and edge environments. Designing lightweight consensus mechanisms—such as Proof of Authority (PoA), Directed Acyclic Graph (DAG)-based approaches, or optimized Practical Byzantine Fault Tolerance (PBFT) variants—could drastically improve scalability and operational sustainability in constrained devices.

iii. Hybrid System Prototyping

Empirical evaluation remains limited. Building and benchmarking hybrid FL–DP–Blockchain prototypes using real-world datasets from domains such as healthcare and finance will be essential for quantifying privacy-utility-latency trade-offs, communication overhead, and energy performance under realistic conditions.

iv. Regulatory Alignment

Integrating privacy-enhancing cryptographic primitives—such as Zero-Knowledge Proofs (ZKPs) and Secure Multi-Party Computation (SMPC)—can bridge the gap between blockchain immutability and compliance with privacy regulations like GDPR and HIPAA. Research in this area should focus on developing regulatory-aware frameworks that automate compliance verification within decentralized learning systems.

v. Cross-Domain Interoperability

Ensuring seamless communication between federated ecosystems across domains (e.g., hospitals, smart cities, and autonomous systems) requires the development of standardized APIs, metadata schemas, and secure communication protocols. This would facilitate interoperability and data exchange without compromising privacy guarantees.

vi. Security Auditing and Explainability

The future of privacy-preserving AI depends not only on protection but also on trust. Embedding explainable AI (XAI) mechanisms within federated architectures will allow transparency in privacy-preserving decisions, support security auditing, and enhance user trust by making model behavior interpretable to stakeholders.

5.3. Final Remarks

In conclusion, Federated Learning augmented by Differential Privacy and Blockchain represents a transformative approach to building trustworthy, privacy-preserving, and regulation-aware AI ecosystems. As data sensitivity and regulatory scrutiny continue to rise, integrating these two paradigms offers a pragmatic pathway toward sustainable decentralized intelligence. Future research that focuses on scalable hybrid architectures, adaptive privacy accounting, and lightweight consensus design, will play a pivotal role in realizing next-generation secure Federated Learning frameworks, capable of empowering Healthcare 5.0, smart industries, and beyond.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S.A. Farooqi, A.A. Rahman, A. Saad, "A Theoretical Comparison of Federated Learning with Differential Privacy and Blockchain for Security and Privacy in IoMT," in Proceedings of the 2025 19th International Conference on Ubiquitous Information Management and Communication, IMCOM 2025, Institute of Electrical and Electronics Engineers Inc., 2025, doi:10.1109/IMCOM64595.2025.10857505.

[2] A. Said, A. Yahyaoui, T. Abdellatif, HIPAA and GDPR Compliance in IoT Healthcare Systems, 198–209, 2024, doi:10.1007/978-3-031-55729-3_16.

[3] S. Ashraf Farooqi, A. Memon, S. Zamir, K. Malik, W. Batool, H. Zahid, NAVIGATING AI IN THE REAL WORLD: TRANSFORMATIONS, REGULATIONS, AND CHALLENGES.

[4] J. Liu, J. Zhang, M.A. Jan, R. Sun, L. Liu, S. Verma, P. Chatterjee, "A Comprehensive Privacy-Preserving Federated Learning Scheme with Secure Authentication and Aggregation for Internet of Medical Things," IEEE Journal of Biomedical and Health Informatics, **28**(6), 3282–3292, 2024, doi:10.1109/JBHI.2023.3304361.

[5] M. Ali, H. Karimipour, M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," Computers and Security, 108, 102355, 2021, doi: 10.1016/j.cose.2021.102355.

[6] K. Begum, M.A.I. Mozumder, M. Il Joo, H.C. Kim, "BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks," Sensors, **24**(14), 2024, doi:10.3390/s24144591.

[7] B. Bhushan, A. Kumar, A.K. Agarwal, A. Kumar, P. Bhattacharya, A. Kumar, Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends, Sustainability (Switzerland), **15**(7), 2023, doi:10.3390/su15076177.

[8] S.A. Farooqi, Federated Learning for Secure and Resilient AI Systems, IGI Global Scientific Publishing: 307–344, 2025, doi:10.4018/979-8-3373-2200-1.ch010.

[9] M. Rahman, H. Jahankhani, Security Vulnerabilities in Existing Security Mechanisms for IoMT and Potential Solutions for Mitigating Cyber-Attacks, 307–334, 2021, doi:10.1007/978-3-030-72120-6_12.

[10] M. Ali, F. Naeem, M. Tariq, G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," IEEE Journal of Biomedical and Health Informatics, **27**(2), 778–789, 2023, doi:10.1109/JBHI.2022.3181823.

[11] S. Rani, A. Kataria, S. Kumar, P. Tiwari, "Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review," Knowledge-Based Systems, 274, 2023, doi:10.1016/j.knosys.2023.110658.

[12] P.M. Mammen, "Federated Learning: Opportunities and Challenges," 2021.

[13] L. Collins, H. Hassani, A. Mokhtari, S. Shakkottai, FedAvg with Fine Tuning: Local Updates Lead to Representation Learning, 2022.

[14] G. Xia, J. Chen, C. Yu, J. Ma, "Poisoning Attacks in Federated Learning: A Survey," IEEE Access, 11, 10708–10722, 2023, doi:10.1109/ACCESS.2023.3.

[15] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, E. Hossain, "Data and Model Poisoning Backdoor Attacks on Wireless Federated Learning, and the Defense Mechanisms: A Comprehensive Survey," IEEE Communications

Surveys & Tutorials, **26**(3), 1861–1897, 2024, doi:10.1109/COMST.2024.3361451.

[16] R. Somasundaram, M. Thirugnanam, "Review of security challenges in healthcare internet of things," Wireless Networks, **27**(8), 5503–5509, 2021, doi:10.1007/s11276-020-02340-0.

[17] A.A. El-Saleh, A.M. Sheikh, M.A.M. Albreem, M.S. Honnurvali, "The Internet of Medical Things (IoMT): opportunities and challenges," Wireless Networks, **31**(1), 327–344, 2025, doi:10.1007/s11276-024-03764-8.

[18] Y. Zhao, J. Chen, "A Survey on Differential Privacy for Unstructured Data Content," ACM Computing Surveys, **54**(10 s), 2022, doi:10.1145/3490237.

[19] J. Shi, W. Wan, S. Hu, J. Lu, L. Yu Zhang, "Challenges and Approaches for Mitigating Byzantine Attacks in Federated Learning," in 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE: 139–146, 2022, doi:10.1109/TrustCom56396.2022.00030.

[20] S.A. Farooqi, A.A. Rahman, A. Saad, "Differential Privacy Based Federated Learning Techniques in IoMT: A Review," in 2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM), IEEE: 1–7, 2024, doi:10.1109/IMCOM60618.2024.10418361.

[21] S.P. Sanon, R. Reddy, C. Lipps, H.D. Schotten, "Secure Federated Learning: An Evaluation of Homomorphic Encrypted Network Traffic Prediction," in 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), IEEE: 1–6, 2023, doi:10.1109/CCNC51644.2023.10060116.

[22] O. Dib, S. Li, Z. Li, R. Abdallah, E. hacen Diallo, "FL-SMPC++: A robust framework for privacy-preserving federated learning," Results in Engineering, 28, 107380, 2025, doi:10.1016/J.RINENG.2025.107380.

[23] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, Z. Tari, "Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey," ACM Computing Surveys, **55**(9), 2023, doi:10.1145/3560816.

[24] H. Xiong, M. Chen, C. Wu, Y. Zhao, W. Yi, Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms, Future Internet, **14**(2), 2022, doi:10.3390/fi14020047.

[25] C. Ma, J. Li, L. Shi, M. Ding, T. Wang, Z. Han, H.V. Poor, "When Federated Learning Meets Blockchain: A New Distributed Learning Paradigm," IEEE Computational Intelligence Magazine, **17**(3), 26–33, 2022, doi:10.1109/MCI.2022.3180932.

[26] Y. Shahsavari, O.A. Dambri, Y. Baseri, A.S. Hafid, D. Makrakis, "Integration of Federated Learning and Blockchain in Healthcare: A Tutorial," 2024.

[27] S.K. Singh, L.T. Yang, J.H. Park, "FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0," Information Fusion, 90, 233–240, 2023, doi:10.1016/J.INFFUS.2022.09.027.

[28] F. Sun, Z. Diao, "Federated Learning and Blockchain-Enabled Intelligent Manufacturing for Sustainable Energy Production in Industry 4.0," Processes, **11**(5), 2023, doi:10.3390/pr11051482.

[29] S. Gupta, "Zero-Knowledge Proofs For Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond," Engineering and Technology Journal, **10**(07), 2025, doi:10.47191/etj/v10i07.23.

[30] H.B. Desai, M.S. Ozdayi, M. Kantarcioglu, "BlockFLA: Accountable Federated Learning via Hybrid Blockchain Architecture," in CODASPY 2021 - Proceedings of the 11th ACM Conference on Data and Application Security and Privacy, Association for Computing Machinery, Inc: 101–112, 2021, doi:10.1145/3422337.3447837.

[31] R. Anitha, M. Murugan, "Privacy-preserving collaboration in blockchain-enabled IoT: The synergy of modified homomorphic encryption and federated learning," International Journal of Communication Systems, **37**(18), 2024, doi:10.1002/dac.5955.

[32] H. Xiong, Y. Zhao, Y. Xia, M. Zhang, K.-H. Yeh, "DA-FL: Blockchain Empowered Secure and Private Federated Learning With Anonymous Authentication," IEEE Transactions on Reliability, **74**(4), 5133–5146, 2025, doi:10.1109/TR.2025.3587088.

[33] H. Chen, S. Huang, D. Zhang, M. Xiao, M. Skoglund, H.V. Poor, "Federated Learning Over Wireless IoT Networks With Optimized Communication and Resources," IEEE Internet of Things Journal, 9(17), 16592–16605, 2022, doi:10.1109/JIOT.2022.3151193.

[34] C. Dwork, Differential Privacy, 1–12, 2006, doi:10.1007/11787006_1.

[35] T. Fukami, T. Murata, K. Niwa, I. Tyou, "DP-Norm: Differential Privacy Primal-Dual Algorithm for Decentralized Federated Learning," IEEE Transactions on Information Forensics and Security, 19, 5783–5797, 2024, doi:10.1109/TIFS.2024.3390993.

[36] F. Ayaz, Z. Sheng, D. Tian, Y.L. Guan, "A Blockchain Based Federated Learning for Message Dissemination in Vehicular Networks," IEEE Transactions on Vehicular Technology, **71**(2), 1927–1940, 2022, doi:10.1109/TVT.2021.3132226.

[37] C. Ying, F. Xia, D.S.L. Wei, X. Yu, Y. Xu, W. Zhang, X. Jiang, H. Jin, Y. Luo, T. Zhang, D. Tao, "BIT-FL: Blockchain-Enabled Incentivized and Secure Federated Learning Framework," IEEE Transactions on Mobile Computing, **24**(2), 1212–1229, 2025, doi:10.1109/TMC.2024.3477616.

[38] S. Feng, M. Mohammady, H. Hong, S. Yan, A. Kundu, B. Wang, Y. Hong, "Harmonizing Differential Privacy Mechanisms for Federated Learning: Boosting Accuracy and Convergence," CODASPY 2025 - Proceedings of the 15th ACM Conference on Data and Application Security and Privacy, 60–71, 2025, doi:10.1145/3714393.3726517.

[39] F. Yu, H. Lin, X. Wang, A. Yassine, M.S. Hossain, "Blockchain-empowered secure federated learning system: Architecture and applications," Computer Communications, 196, 55–65, 2022, doi:10.1016/J.COMCOM.2022.09.008.

[40] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, W. Zhang, "A survey on federated learning: challenges and applications," International Journal of Machine Learning and Cybernetics, **14**(2), 513–535, 2023, doi:10.1007/s13042-022-01647-y.

[41] Z. Cai, J. Chen, Y. Fan, Z. Zheng, K. Li, "Blockchain-Empowered Federated Learning: Benefits, Challenges, and Solutions," IEEE Transactions on Big Data, **11**(5), 2244–2263, 2025, doi:10.1109/TBDATA.2025.3541560.

[42] A. El Ouadrhiri, A. Abdelhadi, "Differential Privacy for Deep and Federated Learning: A Survey," IEEE Access, 10, 22359–22380, 2022, doi:10.1109/ACCESS.2022.3151670.

[43] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," Future Generation Computer Systems, 129, 380–388, 2022, doi:10.1016/J.FUTURE.2021.11.028.

[44] C. Chen, J. Liu, H. Tan, X. Li, K.I.K. Wang, P. Li, K. Sakurai, D. Dou, "Trustworthy federated learning: privacy, security, and beyond," Knowledge and Information Systems, **67**(3), 2321–2356, 2025, doi:10.1007/s10115-024-02285-2.

[45] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, D. Dou, Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning, Knowledge and Information Systems, **66**(8), 4377–4403, 2024, doi:10.1007/s10115-024-02117-3.

[46] B. Soudan, S. Abbas, A. Kubba, O. Abu Waraga, M. Abu Talib, Q. Nasir, "Scalability and performance evaluation of federated learning frameworks: a comparative analysis," International Journal of Machine Learning and Cybernetics, **16**(5), 3329–3343, 2025, doi:10.1007/s13042-024-02453-4.

[47] A.A. Ahmed, O.O. Alabi, "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," IEEE Access, 12, 102219–102241, 2024, doi:10.1109/ACCESS.2024.3429205.

[48] K. Wei, J. Li, C. Ma, M. Ding, C. Chen, S. Jin, Z. Han, H. Vincent Poor, "Low-Latency Federated Learning over Wireless Channels with Differential Privacy," IEEE Journal on Selected Areas in Communications, **40**(1), 290–307, 2022, doi:10.1109/JSAC.2021.3126052.

[49] S. Otoum, I. Al Ridhawi, H. Mouftah, "A Federated Learning and Blockchain-Enabled Sustainable Energy Trade at the Edge: A Framework for Industry 4.0," IEEE Internet of Things Journal, **10**(4), 3018–3026, 2023, doi:10.1109/JIOT.2022.3140430.

[50] S.R. Chalamala, N.K. Kummari, A.K. Singh, A. Saibewar, K.M. Chalavadi, "Federated learning to comply with data protection regulations," CSI Transactions on ICT, **10**(1), 47–60, 2022, doi:10.1007/s40012-022-00351-0.

[51] M. S, J. K R, "Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management," Scientific Reports, **15**(1), 1–20, 2025, doi:10.1038/s41598-025-12225-x.

[52] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, D. Dou, Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning, Knowledge and Information Systems, **66**(8), 4377–4403, 2024, doi:10.1007/s10115-024-02117-3.

[53] A. Hussain, W. Akbar, T. Hussain, A. Kashif Bashir, M.M. Al Dabel, F. Ali, B. Yang, "Ensuring Zero Trust IoT Data Privacy: Differential Privacy in Blockchain Using Federated Learning," IEEE Transactions on Consumer Electronics, **71**(1), 1167–1179, 2025, doi:10.1109/TCE.2024.3444824.

[54] J. Liu, J. Zhang, M.A. Jan, R. Sun, L. Liu, S. Verma, P. Chatterjee, "A Comprehensive Privacy-Preserving Federated Learning Scheme with Secure Authentication and Aggregation for Internet of Medical Things," IEEE Journal of Biomedical and Health Informatics, **28**(6), 3282–3292, 2024, doi:10.1109/JBHI.2023.3304361.

[55] M. Abaoud, M.A. Almuqrin, M.F. Khan, "Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications," IEEE Access, 11(August), 83562–83579, 2023, doi:10.1109/ACCESS.2023.3301162.

[56] N.A. Hussein, H.K. Ben Ayed, Blockchain for Smart Cities Management and Security: A Review, 13–40, 2025, doi:10.1007/978-3-031-69441-7_2.

Copyright: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (https://creativecommons.org/licenses/by-sa/4.0/).