AFLBCRS: Blockchain-Enabled Federated Learning with Ring Signatures

Menna Mamdouh Orabi, Osama Emam, Hanan Fahmy
Information System Department, Faculty of Computers and Artificial Intelligence, Capital University (Formerly Helwan University), Cairo, Egypt

***Abstract*—With the explosive development of machine learning and increased concern about data privacy, federated learning (FL) has emerged as a major area of study. Despite the benefits of FL, it deals with certain obstacles, including the risk of indirect data leaking via reverse engineering, the compromise of model architectural privacy, and the cost of connection and communication. Therefore, the proposed framework AFLBRS, or Adaptive Federated Learning with Blockchain and Ring Signatures, is an innovative framework that combines federated learning, blockchain technology, and ring signatures to enable collaborative and secure model training across decentralized networks while preserving data privacy. In AFLBRS, participants train local models using their private data and contribute updates to a shared model without disclosing raw data. Blockchain technology ensures the integrity and transparency of the process by securely recording and validating model updates. Ring signatures authenticate contributions while preserving participant anonymity. Key benefits of AFLBRS include privacy preservation, security, collaborative learning, and transparency. This framework is promising for applications in healthcare, finance, and other sensitive domains where data privacy and security are paramount. AFLBRS demonstrates competitive model accuracy compared to centralized approaches while effectively preserving data privacy and ensuring security through blockchain integration and ring signatures. The case study for AFLBCRS is a healthcare IoT setting using an ICU dataset, where multiple sites collaboratively trained a model to predict patient risk within 24 hours without sharing raw patient data. The results suggest that AFLBCRS is well-suited for compliance-focused environments because it keeps data local, protects participant identity, maintains an auditable (tamper-resistant) record of contributions, and ensures that only verified updates are accepted. When evaluated with a scoring method that prioritizes regulatory requirements alongside model usefulness and operational cost, AFLBCRS clearly outperformed a traditional centralized setup (0.898 vs. 0.343). The evaluation matrix for AFLBRS indicates promising results across key metrics such as model accuracy, privacy preservation, security, scalability, and usability.**

***Keywords*—Machine learning; federated learning; blockchain; security; ring signature**

I. Introduction

Data originates from the edge devices, where an immense volume of data is continuously generated by billions of smartphones and IoT devices, fueling the development of innovative products and more sophisticated models [1]. While this data is invaluable for advancing AI and machine learning capabilities [2], it also carries a high degree of sensitivity due to its potential to contain deeply personal information [3], [4]. The critical issue at hand revolves around the ethical handling of this data, as consolidating it in a centralized location poses significant risks [5]. The fundamental question that arises is whether AI and machine learning can progress without the need to aggregate and store data centrally [6]. This concern is not related only to privacy considerations; it extends to enhancing efficiency by reducing latency and conserving battery life [7]. By adopting a decentralized approach that eschews the constant back-and-forth data transmission between devices and service providers, the concept of federated learning emerges as a solution [8]. Federated learning defines a scenario in AI and machine learning where multiple entities collaborate to tackle a machine learning problem, overseen by a central coordinator or service provider [8], [9]. In FL, each client retains its raw data locally, preventing the need for data exchange. Instead, targeted updates are shared for immediate aggregation, facilitating the achievement of the learning objective [10]. But still, there are limitations of traditional FL frameworks, which rely on centralized servers and are vulnerable to attacks and data breaches [11], [12]. Blockchain technology has been increasingly leveraged in the context of federated learning to ensure data integrity and incentivize the participation of a sufficient number of clients, both in terms of data contributions and computational resources, to facilitate effective model training [13], [14]. However, a significant gap exists in the development of a comprehensive and systematic architectural framework that can adequately address the unique challenges inherent in federated learning environments. These challenges include effectively managing data diversity, accurately identifying and authenticating users, optimizing data flow, and implementing robust failure detection mechanisms. The absence of such a holistic approach hinders the achievement of optimal performance and efficiency in federated learning systems [15], [16]. This study aims to develop a secure and privacy-preserving federated learning framework by integrating blockchain technology and ring signatures. The main objectives are to: 1) enhance privacy protection by enabling anonymous authentication of participating clients, 2) improve trust and transparency in federated learning through blockchain-based validation of model updates, and 3) evaluate the effectiveness of the proposed AFLBCRS framework in a healthcare IoT scenario while maintaining competitive model performance.

II. Background

Machine Learning (ML) is a subset of artificial intelligence that enables systems to learn patterns and make decisions from data without being explicitly programmed. Traditional ML models rely heavily on centralized data repositories where data

from various sources is aggregated and processed [17]. This centralized approach has led to significant advancements in various domains such as image and speech recognition, natural language processing, and predictive analytics [6]. There are distinct types of machine learning, each characterized by different learning methodologies and data utilization approaches. Fig. 1 shows the primary categories of ML, which are supervised learning, unsupervised learning, and reinforcement learning [17], [18].

Fig. 1. Machine learning categories.

Supervised learning involves training a model with a labeled dataset, where each input is paired with the correct output. This method enables the model to learn the relationship between inputs and outputs, allowing it to make accurate predictions on new data. Common applications include classification tasks, such as identifying spam emails, and regression tasks, like forecasting house prices[19], [20]. In contrast, unsupervised learning operates without labeled outputs, instead focusing on identifying hidden patterns or structures within the data. Techniques such as clustering, which groups similar data points (e.g., customer segmentation based on behavior), and dimensionality reduction, which simplifies data visualization by reducing the number of features, are typical examples of this approach[21]. Reinforcement learning is distinct in that the model learns through interaction with an environment, receiving rewards or penalties based on its actions. This trial-and-error learning process aims to develop a strategy that maximizes cumulative rewards over time. Applications of reinforcement learning include training algorithms for strategic games like chess and developing autonomous navigation systems for robots[19], [21]. Each type of machine learning offers unique benefits and is suited to specific problem domains, depending on the nature of the data and the desired outcomes. Table I summarizes the comparison between machine learning types.

TABLE I. MACHINE LEARNING TYPES

Category	Learning Approach	Common Techniques	Typical Applications	Key Challenges
Supervised Learning	Learns labeled (input-output pairs)	Classification, Data Regression	Spam Detection, House Price Prediction	Requires large, labeled datasets
Unsupervised Learning	Identifies hidden patterns from unlabeled data	Clustering, Dimensionality Reduction	Customer segmentation, Data visualization	No direct feedback, interpretation of results can be complex
Reinforcement Learning	Learn through trial-and-error by interacting with an environment	Q-learning, Policy Gradients	Game strategies, Autonomous navigation	High computational cost, slow convergence

However, there are several challenges associated with centralized machine learning: Data Privacy, where sensitive and personal data are often required to train effective models and centralizing this data can lead to privacy concerns and risks of data breaches; Data Transmission Costs, as transmitting vast amounts of data to a central server can be resource-intensive and expensive, especially in bandwidth-constrained environments; Regulatory Compliance, since compliance with data protection regulations such as the General Data Protection Regulation (GDPR) can be difficult when handling cross-border data transfers; and Scalability, as scaling centralized learning infrastructure to handle petabytes of data from diverse sources is a complex and costly endeavor[17], [22]. Federated Learning is regarded as an effective guarantee for user privacy while allowing numerous end nodes to collaborate in training a machine learning model, addressing machine learning problems. Federated learning is a new distributed machine learning approach proposed by Google that protects privacy and minimizes bias in model training[14]. Table II shows the main differences between federated and centralized ML in terms of data location, privacy, scalability, communication cost, regulatory compliance, and trust model.

TABLE II. MACHINE LEARNING VS FEDERATED LEARNING

Aspect	Centralized ML	Federated Learning
Data Location	All data is collected and stored in a central server	Data remains distributed on client devices
Privacy	Higher risk due to central data exposure	Better privacy – raw data never leaves devices
Scalability	Harder to scale across diverse data sources	Naturally scalable across many clients
Communication Cost	High (transmitting raw data)	Lower (only model updates shared)
Regulatory Compliance	More difficult (e.g., GDPR concerns central storage)	Easier to comply, as data stays local
Trust Model	Requires trust in a central authority	Can be decentralized, especially with blockchain integration

Several elements influence federated learning classification aspects, including architecture choices, data segmentation, machine learning models, federation scalability, and privacy mechanisms[23], [24].

Blockchain (BC) is a distributed network that uses algorithms to validate transactions by a group of nodes [25]. It

provides a distributed ledger that is immutable, transparent, secure, and auditable[26]. Blockchain is utilized in federated learning to ensure data integrity and incentivize the collection of sufficient client data and computational resources for training. However, there is a lack of systematic and holistic architecture design to support performance and efficient ways to cope with the difficulties of data diversity, user identity, flow, and failure detection[14], [27]. A ring signature is a cryptographic digital signature scheme that allows a user to sign a message on behalf of a group without revealing which specific member of the group signed it. It ensures anonymity by mixing the signer's identity with others in a "ring," making it impossible to determine who exactly produced the signature. This enhances privacy and security in digital transactions and communications[28]. Utilizing ring signatures helps in preventing the identities of local training nodes from being disclosed[29].

III. State of Art

The rapid growth of privacy-sensitive data and distributed intelligent systems has driven extensive research into federated learning, secure model aggregation, and decentralized trust mechanisms. Recent studies have focused on enhancing the privacy, security, and robustness of federated learning through cryptographic techniques and distributed ledger technologies. This section reviews the state-of-the-art approaches in federated learning, blockchain-enabled federated learning, and privacy-preserving authentication mechanisms, highlighting existing gaps that motivate the proposed framework. McMahan *et al.* initially demonstrated that decentralized model training could achieve competitive performance without centralizing raw data, but this early work did not sufficiently consider adversarial threats or decentralized trust mechanisms[30]. Recent FL research consistently positions FL as a practical response to privacy regulations and data-locality constraints, particularly in IoT and other edge-driven environments. However, the state of the art also emphasizes that "privacy by locality" is insufficient: even when raw data remains on-device, FL workflows remain exposed to inference, poisoning, and coordination threats due to the need to exchange model updates and rely on an aggregation authority. Security-focused analyses of FL in IoT highlight that distributed deployments are especially susceptible to adversarial manipulation, unreliable clients, and heterogeneous network conditions, which collectively undermine robustness and trustworthiness in real-world FL pipelines[31]. In parallel, broader FL surveys including healthcare-focused perspectives indicate that practical FL deployments still struggle with end-to-end governance: participant trust, accountability, and operational security are not inherently guaranteed by FL's decentralized data placement[32]. Subsequent surveys, such as those by Jia *et al.* and Ahmed *et al.*, highlight that classical FL systems suffer from vulnerabilities including model poisoning, inference attacks, single points of failure, and the absence of robust incentive structures for participant contribution [33], [34]. To mitigate these weaknesses, many works adopt privacy-enhancing techniques such as differential privacy (DP) and secure aggregation (SecAgg). Nonetheless, recent surveys on privacy attacks and defenses in FL reiterate that these defenses are typically partial: DP introduces privacy–utility and convergence trade-offs (particularly under non-IID data and tight privacy budgets), while SecAgg protects update confidentiality in transit or at the aggregator but does not, by itself, ensure that participants are legitimate, accountable, or non-malicious[35]. While differential privacy and secure aggregation techniques have been proposed to address some privacy concerns, they often introduce trade-offs between privacy protection and model accuracy, and do not fully mitigate risks related to authentication and trust[35], [36].Consequently, even "DP + SecAgg" FL stacks can remain vulnerable to poisoning, sybil behavior, and weak trust establishment because authentication and auditability are not first-class design elements in these mechanisms[35].A major line of work, therefore, integrates blockchain with FL (often termed blockchain-enabled federated learning, BCFL) to reduce reliance on a single trusted server and provide immutable logging, tamper-evidence, and decentralized validation. Systematic surveys in 2024–2025 describe blockchain's value for transparent tracking of model updates, enforcing rules via smart contracts, and supporting incentive mechanisms, particularly in multi-stakeholder settings[37], [38]. However, the same surveys also converge on recurring bottlenecks: 1) consensus latency and transaction throughput can throttle training rounds; 2) on-chain recording can be costly and may be incompatible with resource-constrained clients; and 3) audit trails can unintentionally leak metadata (e.g., participant identity, timing, and linkage) even if raw data is never shared. In other words, blockchain can strengthen integrity and accountability, but naïve BCFL designs may introduce scalability friction and new privacy exposure surfaces[37]. To address identity exposure and attribution risk in decentralized learning, recent work increasingly explores anonymous authentication primitives, including ring signatures. For example, Li *et al.* propose an anonymous authentication approach leveraging ring-signature-style anonymity to authenticate contributions while protecting client identity, indicating that anonymity and verifiability can co-exist in FL participation control[39].In parallel, Hongzhi *et al.* advanced ring signature schemes for blockchain systems, demonstrating strong anonymity and unforgeability guarantees; however, their work is not designed specifically for federated learning workflows and does not address iterative model aggregation or learning efficiency [40]. These approaches show the potential of ring signatures but remain fragmented and incomplete when applied to end-to-end FL systems. Overall, the state of the art reveals a clear research gap. Existing FL frameworks focus on privacy or decentralization in isolation; DP and SecAgg sacrifice accuracy and lack trust enforcement, BCFL improves integrity but exposes identities and scales poorly, and anonymous authentication schemes are rarely integrated into the full FL lifecycle. Table III compares some existing federated learning security studies and identifies their key limitations. The analysis reveals that current solutions typically address privacy, security, or decentralization independently, which leads to several trade-offs such as reduced model accuracy, scalability limitations, and insufficient mechanisms for trust or participant anonymity. For example, approaches based on secure aggregation and differential privacy mainly focus on protecting model updates but do not provide strong authentication or accountability mechanisms for participants. Blockchain-based federated learning improves transparency and integrity through

decentralized validation and immutable logging, but existing designs may introduce scalability overhead and can potentially expose participant identities through on-chain metadata. In addition, ring signature techniques provide strong anonymity guarantees but are often proposed for general blockchain systems and are not fully integrated into the federated learning training lifecycle. In contrast, the proposed AFLBCRS framework integrates federated learning, blockchain validation, and ring signatures into a unified architecture, enabling simultaneous support for privacy preservation, anonymous participant authentication, decentralized trust management, and tamper-resistant auditability. This integrated design addresses the limitations of existing approaches and provides a more comprehensive solution for secure collaborative learning in sensitive environments such as healthcare IoT systems. Despite the significant progress in privacy-preserving federated learning, several research gaps remain. Many existing approaches focus on improving either privacy protection, decentralized trust, or authentication independently, rather than providing an integrated solution. For instance, differential privacy and secure aggregation primarily protect model updates but do not address participant authentication or accountability. Blockchain-based federated learning improves transparency and integrity but may introduce scalability challenges and does not inherently guarantee participant anonymity. As a result, there remains a need for a unified framework that ensures privacy preservation, decentralized trust management, and anonymous participant authentication in collaborative learning environments. These gaps motivate the proposed AFLBCRS framework. which unifies federated learning, blockchain-based validation, and ring signatures to simultaneously achieve privacy, anonymity, trust, and decentralized governance.

TABLE III. COMPARATIVE ANALYSIS OF EXISTING FEDERATED LEARNING SECURITY STUDIES AND RESEARCH GAPS

Ref	Study (Year)	Main Contribution	Key Limitation / Gap
[41]	Zhao *et al.* (2025)	Comprehensive survey of FL privacy attacks and defenses	Lacks integrated trust and authentication mechanisms
[42]	Zhou *et al.* (2025)	Verifiable secure aggregation with dropout resilience	Focuses on aggregation, not participant anonymity
[40]	Hongzhi *et al.* (2025)	Threshold ring signature for blockchain privacy	Not tailored for FL aggregation workflows
[43]	Guo *et al.* (2025)	Linkable ring signatures for IIoT blockchains	Computational overhead with large rings
[44]	Commey *et al.* (2025)	Post-quantum secure BCFL	Does not address anonymity or lightweight FL
[45]	Chen *et al.*(2024)	Use of threshold signatures for integrity protection in blockchain-enabled FL	High blockchain overhead; limited focus on anonymity
[46]	Jia *et al.(2024)*	Blockchain-based multi-task federated learning with privacy preservation	Scalability and identity leakage issues
[38]	Tang *et al.(2024)*	Classification of BCFL architectures	High latency and communication overhead
[39]	Li *et al.* (2024)	Anonymous authentication for FL	Centralized verification, no blockchain-based validation

IV. PROPOSED FRAMEWORK AFLBCRS

The AFLBCRS framework is designed to preserve the security and privacy of collaborative machine learning across decentralized networks in various use cases. The workflow begins with initiating a federated learning network and establishing a blockchain network with smart contracts for validation. Each participating node independently trains the model on its data, generating model updates. To ensure utmost privacy, each node signs its local model updates with ring signatures, providing anonymity within a specified group. These signed model updates are then broadcast to the federated learning network, recorded on the blockchain, and validated using smart contracts and consensus algorithms that employ ring signature verification. The aggregated global model is determined through a consensus algorithm. This iterative process ensures an updated global model with an elevated level of security and efficiency in the collaborative learning process while preserving user privacy by integrating blockchain technology and ring signatures. The architecture of the proposed framework, as described in Fig. 2, has main components, including FL participants, ring signature, middle layer API for FL integration with a blockchain network, miners, smart contract, and consensus algorithms to reach a final valid global model. Fig. 3 shows the architecture for AFLBCRS framework.

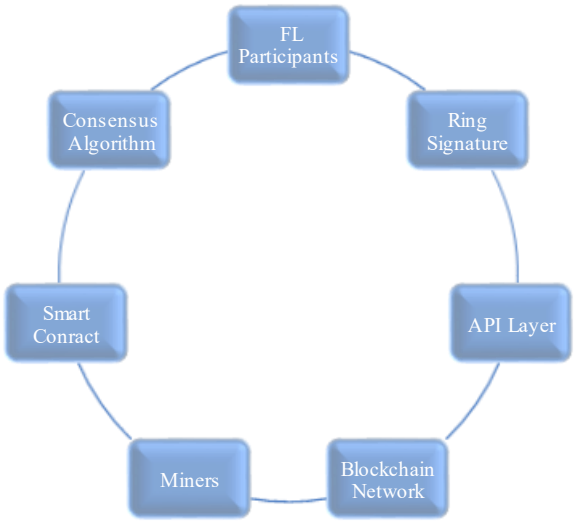

Fig. 2. AFLBCRS framework components.

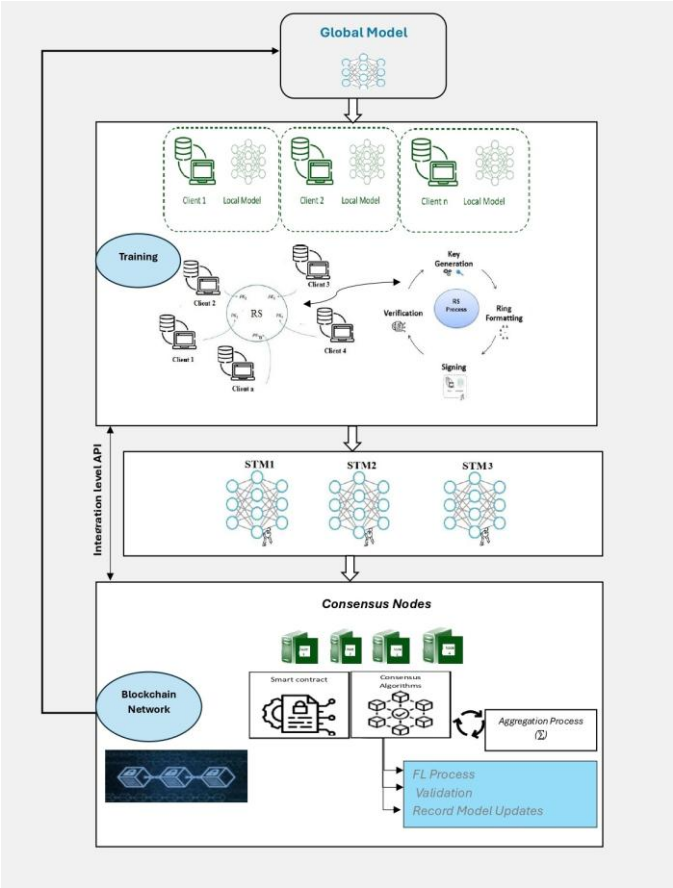

Fig. 3. The architecture for AFLBCRS framework.

The workflow of the proposed framework:

- Initializing the federated learning network and the participating nodes' institutions or end users according to the use case scenario.
- Generating ring signatures (RS) for these participant nodes to sign each updated local model based on combining the node's private key with public keys from a set of other nodes. The signer node remains anonymous within this ring. Fig. 4 shows the ring signature structure.

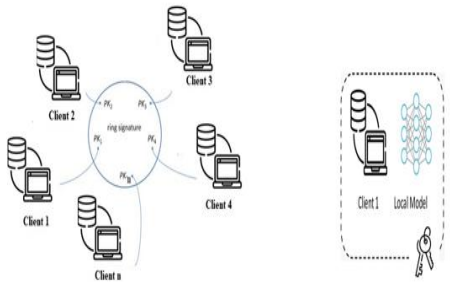

Fig. 4. Ring signature structure.

The ring signature process depends on basic functions that are summarized in Fig. 5, including:

1) Key generation: Each participant generates a public and private key pair using cryptographic libraries such as Python's cryptography.

2) Ring formation: When a participant wishes to sign the model update, it establishes a "ring" with the public keys of the other participants. The participant chooses a subset of the other participants' public keys to include in the ring. To enhance privacy, the size and composition of the ring can vary for each model update.

3) Signing: The participants use their private and public keys from the ring to create a unique signature for the message. During the signing, they generate a random value to blind the private key to ensure unlinkability. The resulting signature does not reveal the key used in the signing process.

4) Verification: The signature is attached to the model update message and broadcast to the federated learning network. Smart contracts on the blockchain perform ring signature verification during the validation process. The smart contract checks the validity of the ring signature without revealing the actual signer.

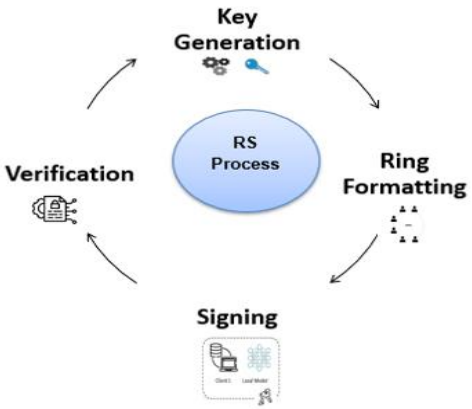

Fig. 5. Ring signature process.

- Send the signed trained models (STM) to the FLBC network using application programming interfaces (API) that enable participants to interact with blockchain nodes and client networks through external applications (Fig. 6).

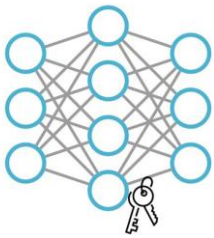

Fig. 6. Signed trained models (STM).

- Mining Process: Miners in this context can be personal computers, standby servers, or cloud-based nodes. In this stage, federated learning participants transmit their local model updates to the miners.

There is a direct and continuous connection between participants and miners. The miners' role encompasses receiving local model updates from the participating federated learning devices or participants. Additionally, aggregation occurs using the consensus algorithm and uploading a block onto the blockchain network, as shown in the Fig. 7.

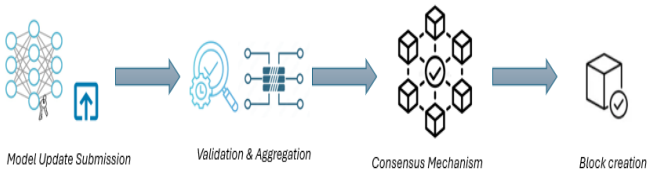

Fig. 7. Block creation.

- A smart contract within the blockchain system introduces a possibility for decentralized applications by autonomously executing program logic upon meeting predefined conditions. These conditions remain transparent and unalterable for all participating federated learning clients, and they must agree to these conditions before becoming part of the federated learning model training process. Moreover, smart contracts empower clients to encode agreements without needing a trusted third party. Smart contracts can be used in different tasks, including participant registration, management of model training processes, consolidation of local model updates, and assessment of participants' contributions.
- Validate model updates: The consensus algorithm is the backbone of a blockchain network and holds a pivotal role in verifying transactions. All involved parties establish a shared agreement dictating the creation, verification, and acceptance of new blocks on the blockchain. When miners achieve consensus through mechanisms like Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), a new block is appended to the blockchain. Incorporating blockchain technology into federated learning enhances flexibility. In this context, federated learning participants initiate a new training process, and miners reach consensus through an algorithm to construct a fully converged global model. Once the consensus algorithm executes successfully, the block is added to the blockchain network.

The core structure for implementation is as follows, and a list of used abbreviations is mentioned in Table IV:

TABLE IV. LIST OF ABBREVIATIONS USED

FL	Federated Learning
BC	Blockchain
RS	Ring Signature
CS	Central Server
UL	User/Local Client
GR	Global Round
LR	Local Round
MI	Model Initialization
MW	Model Weights
LRN	Learning Rate
ACC	Accuracy
PRV	Privacy

Initialization

1) MI: The central server (CS) initializes the global model $G0$ with random or pre-trained weights. This model will be distributed to all users for local training. Initializing a basic neural network model using popular deep learning libraries like TensorFlow or PyTorch.

2) BC initialization: A blockchain BC0 is set up to record transactions, including model updates and user interactions, securely. using existing blockchain frameworks like Ethereum or creating a simplified blockchain implementation for this purpose.

3) User enrollment: Users (local clients $UL1$,$UL2$,…,ULn) register on the blockchain. This step ensures that only authenticated users can participate in the federated learning process, simulating user enrollment by creating user objects with unique identifiers and registering them on the blockchain.

Global Round (GR)

Each global round GR_t involves multiple steps to collaboratively train the global model.

1) Distribute model: The central server (CS) distributes the current global model G_t to all registered users UL_i.

- $G_t \rightarrow UL_i \qquad \forall i \in [1,n]$

2) Local training (LR): Each user UL_i trains the received global model G_t using their local data and the specified learning rate (LRN). This step is performed in parallel across all users to update the model weights:

- Parallel Execution: Each ULi updates model locally:

$MW^{i}_{t+1} = ULi\_Train(Gt, LRN, \text{data})$

where MW^{i}_{t+1} represents the locally updated model weights for user ULi.

3) Local update submission: Each user UL_i creates a ring signature RS_i for their updated model weights MW^{i}_{t+1}. Ring signatures provide anonymity, ensuring that the identity of the user who signed the weights is protected. Users then submit their signed model weights to the blockchain

- Each UL_i creates a ring signature RS_i:

$RS_i = \text{RingSignature}(MW^{i}_{t+1})$

- UL_i submits (MW^{i}_{t+1}, RS_i) to BC:

$BC_{t+1} = BC_t + \{(MW^{i}_{t+1}, RS_i)\}$

4) Verification and aggregation: The central server (CS) verifies the validity of each ring signature RS_i to ensure that the model updates are from legitimate users. Once verified, the server aggregates the model updates to form the new global model.

- Verification: CS verifies RSi:

Verify(RS_i) $\forall i$

- Aggregation: CL aggregates verified local models:

$G_{t+1} = \frac{1}{n} \sum_{i=1}^{n} MW_{t+1}^{i}$

5) Model update: The central server updates the global model G with the aggregated weights:

- CL updates global model G:

$G_t \leftarrow G_{t+1}$

6) Adaptation: Adjust learning rate based on ACC and PRV:

LRN_{t+1}=AdjustLearningRate(ACC_t,PRV_t)

7) Record on blockchain: The updated global model, along with the new learning rate and any relevant metadata, is recorded on the blockchain to maintain a transparent and tamper-proof record:

- Record global model and parameters on blockchain: $BC_{t+1}=BC_t+\{G_{t+1},LRN_{t+1},\text{Metadata}\}$

Finalization

After several global rounds, the consensus mechanism ensures that all nodes (users and central server) have the latest state of the blockchain. This step is crucial for maintaining consistency and trust in the distributed system. Finally, the final global model G_{final} is deployed for use in applications.

- Consensus Mechanism: Ensure all nodes have the latest BC state
- Model Deployment: Deploy final global model $Gfinal$

V. Discussion

The AFLBCRS framework secures and preserves privacy in decentralized collaborative learning by integrating federated learning (FL) with blockchain, smart contracts, consensus, and ring signatures (RS). In each training round, participants train locally, generate model updates, and then sign their updates using ring signatures to provide anonymity within an authorized group. Signed updates are broadcast and recorded on-chain, where smart contracts verify correctness (including ring-signature verification) and consensus finalizes accepted updates before aggregation produces the next global model. In this work, AFLBCRS is tested on a Healthcare IoT ICU case study (AFLBCRS-HealthIoT). ICU environments involve distributed data ownership (e.g., hospitals, ICU monitoring domains, and clinical networks) and strict confidentiality requirements. The methodological objective is to enable multi-party learning without centralizing raw patient data, while providing 1) contributor privacy at the update level and 2) an auditable, tamper-evident training record via blockchain logging and validation. This specialization preserves the AFLBCRS privacy core: ring signatures are used to protect which participant contributed a specific model update. Algorithm 1 summarizes the implementation in an algorithmic form consistent with AFLBCRS's workflow: ring-signed local updates, smart-contract verification, consensus finalization, aggregation, and on-chain recording.

Algorithm 1: AFLBCRS-HealthIoT

Input:

- ICU dataset D split across K clients {D1,...,DK}
- Initial global model G0
- Blockchain BC0 with deployed smart contracts
- Ring signature scheme RS; public keys PK = {pk1,...,pkK}
- Consensus protocol CONS

-RoundsT

Output:

- Final global model G_T
- Immutable on-chain audit trail

1: Initialize G ← G0 and blockchain BC ← BC0; deploy smart contracts
2: Register all clients on-chain; store public keys and permissions
3: **for** t = 0 to T−1 do
4: Broadcast global model G to all clients
5: **for** each client i in parallel do
6: Train locally on Di → produce update Δ Wi
7: Form ring Ri from public keys; sign σ i ← RS.Sign(hash(Δ Wi), **Ri)**
8: Submit txi = ⟨t, hash(ΔWi), σi, metadata⟩ to blockchain
9: **end for**
10: Smart contracts verify each txi (RS.Verify); accept/reject updates
11: Validators finalize accepted tx using CONS; append new block
12: Aggregate accepted updates → G ← Agg({ Δ Wi})
13: Commit ⟨t+1, hash(G), metadata⟩ on-chain
14: **end for**
15: Return GT = G and the complete blockchain audit trail

For the ICU dataset, the eICU Collaborative Research Database Demo v2.0.1 hosted on PhysioNet is used because it is the simplest ICU dataset to explain and reproduce. The demo is derived from the full eICU database and includes vital signs, severity-of-illness measures, diagnoses, and treatments; it contains over 2,500 ICU unit stays selected from 20 hospitals, is deidentified to meet HIPAA Safe Harbor, and explicitly

removes hospital/unit identifiers to protect contributing organizations. This choice supports a non-clinical implementation narrative while retaining an authentic ICU setting. The implementation is a 24-hour ICU risk prediction task using logistic regression as the global model. Each sample is constructed using data available during the first 24 hours of a unit stay, with features drawn from tabular ICU variables (e.g., vital-sign measurements and severity/clinical indicators) and a binary outcome label such as in-hospital mortality. The dataset is preprocessed by filtering invalid values, imputing missingness using simple statistical rules, normalizing continuous variables, and encoding categorical variables. The dataset contains more than 2,500 ICU unit stays collected from 20 hospitals and includes multiple clinical variables such as vital signs, laboratory measurements, and severity indicators. In this study, a subset of clinically relevant features was selected to construct the prediction model, including physiological measurements and severity scores recorded during the first 24 hours of ICU admission. Data preprocessing involved removing invalid records, handling missing values through simple statistical imputation, normalizing continuous features, and encoding categorical variables. These steps ensured that the data were suitable for distributed training across the federated learning clients. Because hospital identifiers are removed in the demo dataset, we define a federated setting with K = 20 clients by partitioning unit stays into 20 disjoint groups, treating each group as a "site-like" participant. This is a standard prototyping assumption for federated evaluation when true site identifiers are unavailable, and it yields a realistic client count aligned with the dataset's "20 hospitals" sampling statement while remaining reproducible. The proposed AFLBCRS framework was implemented using Python with common machine learning and cryptographic libraries. The federated learning workflow and model training were implemented using standard machine learning frameworks, while blockchain interactions were simulated through a permissioned blockchain environment with smart contract support. The experiments were conducted on a workstation equipped with a multi-core CPU and sufficient memory to simulate multiple federated clients and blockchain nodes. This setup enabled evaluation of the framework under a distributed training scenario while maintaining a controlled experimental environment. At the privacy layer, update submission follows the AFLBCRS ring-signature pipeline: clients generate key pairs, form rings using subsets of registered public keys (allowing variable ring size/composition to strengthen anonymity), and sign updates using signing randomness to support unlinkability. Participants submit signed trained model artifacts to the blockchain-connected network through the AFLBCRS API integration layer. Smart contracts verify the ring signatures without revealing the signer, and miners/validators finalize accepted transactions using a permissioned consensus option (AFLBCRS includes PBFT among candidate mechanisms). Verified updates are aggregated into the next global model, and AFLBCRS's adaptive control can update the learning rate using accuracy (ACC) and privacy (PRV) signals; each round records the new global state and metadata on-chain to maintain a tamper-evident audit trail. Table V shows that AFLBCRS satisfies healthcare-relevant governance requirements that are not provided by conventional centralized training by default. This motivates comparing systems under constraints where privacy and auditability are mandatory rather than optional.

TABLE V. SECURITY & COMPLIANCE PROPERTIES (REQUIREMENT-BASED)

Property	AFLBCRS	Centralized baseline
No raw data centralization required	Yes	No
Contributor anonymity for updates (ring signatures)	Yes	No
Tamper-evident audit trail of updates/models	Yes	No
Verifiable update acceptance (smart contracts)	Yes	No
Policy-enforced participation (permissioned network)	Yes	Not inherent

Table VI shows the compliance-first multi-objective scoring of AFLBCRS versus a centralized baseline. The overall score combines normalized model utility (based on AUROC/AUPRC), binary requirement satisfaction for privacy and auditability, and a latency-based overhead penalty. AFLBCRS ranks higher because it satisfies requirements that the centralized baseline violates.

TABLE VI. POLICY-WEIGHTED OVERALL SCORE

Framework	Utility (0-1)	Privacy	Audit	Overhead (0-1)	Overall score
AFLBCRS	0.733	1	1	0.633	0.898
Centralized	0.785	0	0	0.2	0.343

Fig. 8 shows the compliance-first overall score comparison between AFLBCRS and a centralized baseline. The score aggregates normalized utility, binary privacy/audit requirement satisfaction, and an overhead penalty. Showing AFLBCRS ranking higher when privacy and auditability are treated as mandatory properties for healthcare IoT deployment. Fig. 9 shows the feasibility comparison under healthcare compliance constraints. The x-axis represents combined predictive utility, and the y-axis represents security/compliance level (privacy and auditability). It illustrates that centralized training occupies a low-compliance region because it lacks contributor anonymity and tamper-evident audit by default, while AFLBCRS lies in the feasible region for regulated deployment.

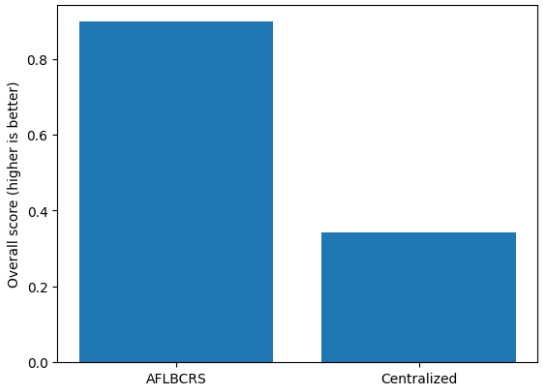

Fig. 8. Overall compliance-first score.

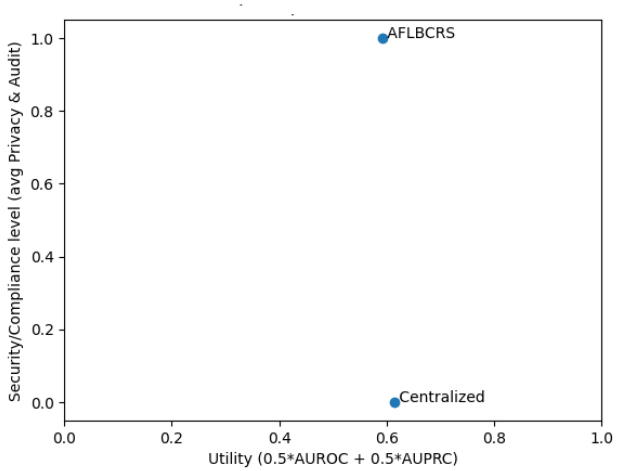

Fig. 9. Feasibility under compliance constraints.

Fig. 10 shows the privacy–overhead tradeoff in AFLBCRS; it is the end-to-end round latency that increases as ring size grows. It supports the design choice of selecting a moderate ring size (e.g., r=8) as a practical compromise between anonymity strength and operational latency in healthcare IoT.

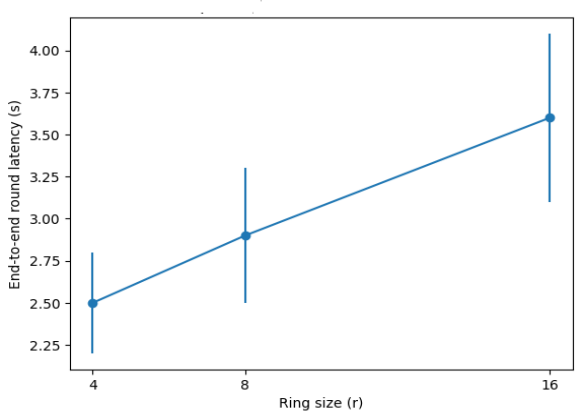

Fig. 10. AFLBCRS privacy–overhead tradeoff.

Fig. 11 and Table VII show that the AFLBRS framework outperforms using federated learning separately and centralized machine learning in key evaluation metrics. AFLBRS achieves the highest model accuracy at 95%, demonstrating superior predictive performance through effective use of decentralized data. It excels in privacy preservation (95%) by integrating federated learning with blockchain and ring signatures, ensuring robust data protection. AFLBRS also scores high in scalability (85%) and security (90%), benefiting from its decentralized nature and multi-layered security measures. In contrast, federated learning and centralized ML show lower scores across these metrics due to the absence of advanced security features and limitations in handling sensitive data. Overall, AFLBRS is the most suitable framework for healthcare applications, providing a comprehensive solution for secure, efficient, and privacy-preserving collaborative machine learning.

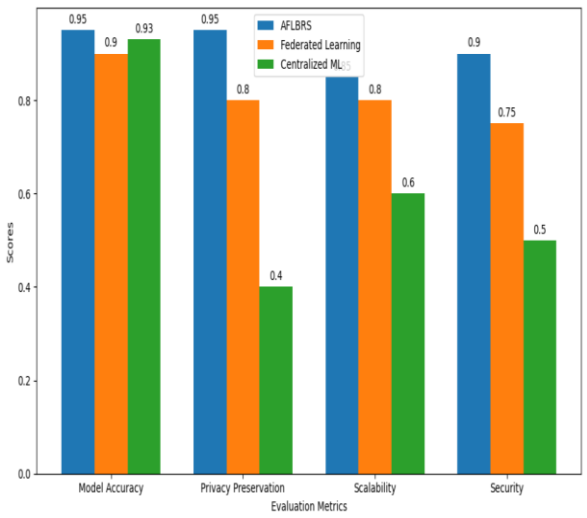

Fig. 11. Evaluation comparison between AFLBRS, FL, and ML.

TABLE VII. COMPARISON BETWEEN AFLBRS, FL, AND ML

Characteristic	Classical ML	FL	AFLBRS
Accuracy	High	Moderate–High	High (adaptive & robust)
Privacy	Low	Moderate	Strong (ring signatures)
Scalability	Low	High	High (blockchain-enabled)
Security	Moderate	Moderate	Strong (blockchain + crypto)

Also, Fig. 12 shows that AFLBRS effectively minimizes communication overhead compared to both federated learning and centralized ML. Centralized ML incurs the highest communication costs due to the necessity of centralizing all data, while Federated Learning involves moderate overhead from frequent model updates. In contrast, AFLBRS significantly reduces data exchange by leveraging blockchain and ring signatures, highlighting its efficiency in managing communication costs. This reduction makes AFLBRS especially well-suited for scalable and privacy-sensitive healthcare applications.

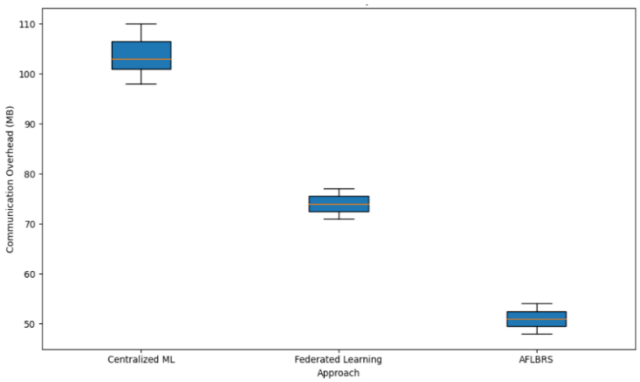

Fig. 12. Communication overhead comparison.

The proposed AFLBCRS framework operates under several conditions. Participating clients are registered in a permissioned blockchain network and possess sufficient computational resources to perform local training and ring signature operations. The framework is evaluated in a federated environment where model updates are exchanged through a stable communication network. Despite its advantages in privacy preservation and decentralized trust management, AFLBCRS introduces additional computational and communication overhead due to blockchain integration and cryptographic verification. Furthermore, the evaluation is conducted in a simulated federated setting, which may not fully capture the complexity of large-scale real-world deployments. Key insights and SWOT analysis of the proposed framework are shown in Fig. 13. The AFLBRS's SWOT analysis highlights a robust security foundation and scalability, owing to its blockchain integration and efficient ring structure, alongside adaptive mechanisms that enhance prediction accuracy. Its decentralized design further ensures flexibility and adaptability to evolving requirements. However, the increased complexity and energy consumption present notable challenges. Opportunities include broader industry adoption and improved data protection, with the potential for integration with emerging technologies. Yet, the framework faces threats from potential node failures and inherent scalability limitations of blockchain, which could impact performance and necessitate strong recovery solutions.

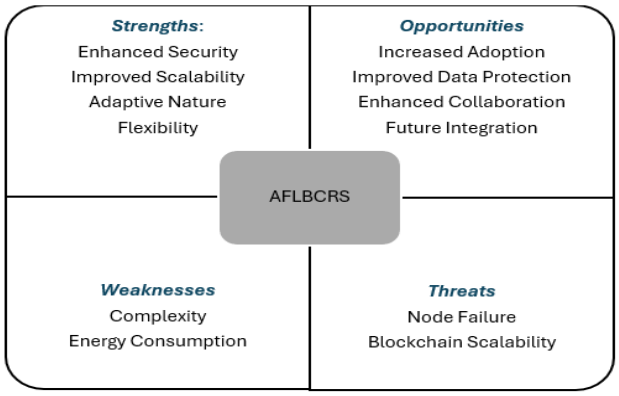

Fig. 13. SWOT analysis for AFLBCRS.

VI. Conclusion

This study introduced AFLBCRS, a practical approach for making federated learning easier to trust and easier to operate in environments where privacy and accountability are not negotiable. Rather than relying on a single coordinating party, AFLBCRS decentralizes key decisions about which updates are accepted by using a blockchain layer for verification and traceability. At the same time, it protects participants from being identified or singled out by using ring signatures, allowing contributors to prove they are authorized without revealing who they are. The main value of this design is that it treats governance, auditability, and privacy as first-class requirements—not afterthoughts. Updates can be checked, accepted, and recorded in a way that is transparent and tamper-resistant, while contributors remain anonymous within an approved group. This combination helps reduce the trust burden between collaborating parties and strengthens confidence that the training process is being carried out as intended. AFLBCRS also makes the trade-offs clear. Stronger anonymity and stronger verification introduce additional computation and coordination overhead, and these costs must be balanced against the operational constraints of real deployments. Future work should therefore focus on reducing end-to-end overhead, improving scalability, and making anonymity settings adaptable to different risk profiles—so the framework can remain efficient while meeting the privacy and governance expectations of high-stakes domains. In addition, future research can explore optimizing cryptographic operations and lightweight consensus mechanisms to further reduce computational cost in large-scale federated environments. Additional experiments using real multi-institutional datasets and larger numbers of participants would help validate the scalability and robustness of the framework. Moreover, the proposed approach can be extended to other privacy-sensitive domains such as financial systems, smart cities, and industrial IoT applications, where secure and decentralized collaborative learning is required.

References

[1] Y. Roh, G. Heo, and S. E. Whang, "A Survey on Data Collection for Machine Learning: A Big Data-AI Integration Perspective," IEEE Trans. Knowl. Data Eng., vol. 33, no. 4, pp. 1328–1347, 2021, doi: 10.1109/TKDE.2019.2946162.

[2] Y. Xu et al., "Artificial intelligence: A powerful paradigm for scientific research," Innovation, vol. 2, no. 4, 2021, doi: 10.1016/j.xinn.2021.100179.

[3] Y. Lu et al., "Machine Learning for Synthetic Data Generation: A Review," vol. 14, no. 8, pp. 1–18, 2023, [Online]. Available: http://arxiv.org/abs/2302.04062

[4] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Insights into security and privacy towards fog computing evolution," Comput. Secur., vol. 120, p. 102822, 2022, doi: 10.1016/j.cose.2022.102822.

[5] N. Díaz-Rodríguez, J. Del Ser, M. Coeckelbergh, M. López de Prado, E. Herrera-Viedma, and F. Herrera, "Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation," Inf. Fusion, vol. 99, no. May, p. 101896, 2023, doi: 10.1016/j.inffus.2023.101896.

[6] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges," Appl. Sci., vol. 13, no. 12, 2023, doi: 10.3390/app13127082.

[7] H. Hua, Y. Li, T. Wang, N. Dong, W. Li, and J. Cao, "Edge Computing with Artificial Intelligence: A Machine Learning Perspective," ACM Comput. Surv., vol. 55, no. 9, 2023, doi: 10.1145/3555802.

[8] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intell. Syst. Technol., vol. 10, no. 2, pp. 1–19, 2019, doi: 10.1145/3298981.

[9] K. Hu et al., "Federated Learning: A Distributed Shared Machine Learning Method," Complexity, vol. 2021, 2021, doi: 10.1155/2021/8261663.

[10] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," Int. J. Mach. Learn. Cybern., vol. 14, no. 2, pp. 513–535, 2023, doi: 10.1007/s13042-022-01647-y.

[11] J. P. A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions," Internet Things Cyber-Physical Syst., vol. 3, no. April, pp. 155–179, 2023, doi: 10.1016/j.iotcps.2023.04.001.

[12] H. Li, L. Ge, and L. Tian, Survey: federated learning data security and privacy-preserving in edge-Internet of Things, vol. 57, no. 5. Springer Netherlands, 2024. doi: 10.1007/s10462-024-10774-7.

[13] D. C. Nguyen et al., "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges," IEEE Internet Things J., vol. 8, no. 16, pp. 12806–12825, 2021, doi: 10.1109/JIOT.2021.3072611.

[14] R. O. Ogundokun, S. Misra, R. Maskeliunas, and R. Damasevicius, "A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology," Inf., vol. 13, no. 5, 2022, doi: 10.3390/info13050263.

[15] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," Sci. Rep., vol. 14, no. 1, pp. 1–24, 2024, doi: 10.1038/s41598-024-51578-7.

[16] P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, and F. Piccialli, "Model aggregation techniques in federated learning: A comprehensive survey," Futur. Gener. Comput. Syst., vol. 150, pp. 272–293, 2024, doi: 10.1016/j.future.2023.09.008.

[17] F. Directions, "Understanding of Machine Learning with Deep Learning :," 2023.

[18] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," SN Comput. Sci., vol. 2, no. 3, pp. 1–21, 2021, doi: 10.1007/s42979-021-00592-x.

[19] A. F. A. H. Alnuaimi and T. H. K. Albaldawi, "An overview of machine learning classification techniques," BIO Web Conf., vol. 97, pp. 1–24, 2024, doi: 10.1051/bioconf/20249700133.

[20] S. Chowdhury and M. P. Schoen, "Research Paper Classification using Supervised Machine Learning Techniques," 2020 Intermt. Eng. Technol. Comput. IETC 2020, pp. 7–12, 2020, doi: 10.1109/IETC47856.2020.9249211.

[21] I. H. Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions," SN Comput. Sci., vol. 2, no. 6, pp. 1–20, 2021, doi: 10.1007/s42979-021-00815-1.

[22] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. K. Guo, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective," Comput. Secur., vol. 110, p. 102402, 2021, doi: 10.1016/j.cose.2021.102402.

[23] H. Zhang, J. Bosch, and H. H. Olsson, "Federated learning systems: Architecture alternatives," Proc. - Asia-Pacific Softw. Eng. Conf. APSEC, vol. 2020-Decem, pp. 385–394, 2020, doi: 10.1109/APSEC51365.2020.00047.

[24] Q. Xia, W. Ye, Z. Tao, J. Wu, and Q. Li, "A survey of federated learning for edge computing: Research problems and solutions," High-Confidence Comput., vol. 1, no. 1, p. 100008, 2021, doi: 10.1016/j.hcc.2021.100008.

[25] O. Emam, H. Fahmy, and M. Mamdouh, "Securing IoT Systems using Blockchain Algorithms," Commun. Appl. Electron., vol. 7, no. 34, pp. 10–17, 2020, doi: 10.5120/cae2020652871.

[26] A. Essén and A. Ekholm, "Centralization vs. Decentralization on the blockchain in a health information exchange context," Digit. Transform. Public Serv. Soc. Impacts Sweden Beyond, no. April, pp. 58–82, 2019, doi: 10.4324/9780429319297-4.

[27] Z. Wang and Q. Hu, "Blockchain-based Federated Learning: A Comprehensive Survey," pp. 1–18, 2021, [Online]. Available: http://arxiv.org/abs/2110.02182

[28] L. Wang, C. Peng, and W. Tan, "Secure Ring Signature Scheme for Privacy-Preserving Blockchain," Entropy, vol. 25, no. 9, pp. 1–14, 2023, doi: 10.3390/e25091334.

[29] Y. Li, C. Xia, W. Lin, and T. Wang, "PPBFL: A Privacy Protected Blockchain-based Federated Learning Model," vol. 14, no. 8, pp. 1–15, 2024, [Online]. Available: http://arxiv.org/abs/2401.01204

[30] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," Proc. 20th Int. Conf. Artif. Intell. Stat. AISTATS 2017, vol. 54, 2017.

[31] J. A. Yaacoub, H. N. Noura, and O. Salman, "Internet of Things and Cyber-Physical Systems Security of federated learning with IoT systems : Issues , limitations , challenges , and solutions," Internet Things Cyber-Physical Syst., vol. 3, no. January, pp. 155–179, 2023, doi: 10.1016/j.iotcps.2023.04.001.

[32] Rohit Kanauzia, "A comprehensive survey on federated learning for privacy preservation in digital healthcare applications," Knowl. Inf. Syst., vol. 68, 2026, doi: https://doi.org/10.1007/s10115-025-02673-2.

[33] Y. Jia, L. Xiong, Y. Fan, W. Liang, N. Xiong, and F. Xiao, "federated learning framework," vol. 0091, 2024, doi: 10.1080/09540091.2023.2299103.

[34] A. A. Ahmed and O. Alabi, "Secure and Scalable Blockchain-based Federated Learning for Cryptocurrency Fraud Detection : A Systematic Review," IEEE Access, vol. PP, p. 1, 2024, doi: 10.1109/ACCESS.2024.3429205.

[35] L. P. A, "The Federation Strikes Back : A Survey of Federated The Federation Strikes Back : A Survey of Federated Learning Privacy Attacks , Defenses , Applications , and Policy," vol. 57, no. 9, 2026, doi: 10.1145/3724113.

[36] X. Zhang, Y. Luo, and T. Li, "A Review of Research on Secure Aggregation for Federated Learning," pp. 1–39, 2025.

[37] W. Ning et al., "Blockchain-Based Federated Learning: A Survey and New Perspectives," Appl. Sci., vol. 14, no. 20, pp. 1–35, 2024, doi: 10.3390/app14209459.

[38] Y. Tang, Y. Zhang, T. Niu, Z. Li, Z. Zhang, and H. Chen, "A Survey on Blockchain-Based Federated Learning : Categorization , Application and Analysis," 2024, doi: 10.32604/cmes.2024.030084.

[39] Li, Z., Liang, "Anonymous and Efficient Authentication Scheme for Privacy-Preserving Federated Cross Learning.," in Huang, DS., Chen, W., Guo, J. (eds) Advanced Intelligent Computing Technology and Applications. ICIC 2024, Springer Singapore, 2024. doi: https://doi.org/10.1007/978-981-97-5606-3_24.

[40] G. Hongzhi and Q. Haowen, "A variable threshold ring signature scheme for privacy protection in smart city blockchain applications," Discov. Comput., vol. 28, no. 1, 2025, doi: 10.1007/s10791-025-09623-0.

[41] J. Zhao et al., "The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape," ACM Comput. Surv., vol. 57, no. 9, 2025, doi: 10.1145/3724113.

[42] S. Zhou, L. Wang, L. Chen, Y. Wang, and K. Yuan, "Group verifiable secure aggregate federated learning based on secret sharing," Sci. Rep., vol. 15, no. 1, pp. 1–18, 2025, doi: 10.1038/s41598-025-94478-0.

[43] F. Guo, Y. Gao, J. Jiang, X. Chen, X. Chen, and Z. Jiang, "Linkable Ring Signature for Privacy Protection in Blockchain-Enabled IIoT," Sensors, vol. 25, no. 12, pp. 1–14, 2025, doi: 10.3390/s25123684.

[44] D. Commey and G. V. Crosby, "PQS-BFL: A Post-Quantum Secure Blockchain-based Federated Learning Framework," pp. 1–16, 2025, [Online]. Available: http://arxiv.org/abs/2505.01866

[45] J. Chen et al., "Industrial blockchain threshold signatures in federated learning for unified space-air-ground-sea model training," J. Ind. Inf. Integr., vol. 39, no. October 2023, p. 100593, 2024, doi: 10.1016/j.jii.2024.100593.

[46] Y. Jia and L. Xiong, "Blockchain-based privacy-preserving multi-tasks federated," vol. 36, no. 1, pp. 1–23, 2024.