

A Survey on Secure Blockchain-Based Federated Learning for Privacy-Preserving Data Sharing and Protection Against Unauthorized Access

Aruna S. Kamble^{1,2*} and
Dr. Ekta Sarda¹

¹Department of Computer Engineering, Ramrao Adik Institute of Technology, Deemed to be University, Nerul, Navi Mumbai 400706, India

²Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai 400614, India

*E-mail: aruna.s.kamble@gmail.com

Received for publication
August 01, 2025.

Abstract

The integration of blockchain with federated learning (FL) has emerged as a promising solution to several challenges in Machine Learning (ML), particularly for decentralized data processing across diverse domains. This survey explores the application of this integrated approach in health care, smart cities, smart agriculture, smart grids, and other applications. The blockchain ensures privacy and integrity of medical data in health care and smart cities, while challenges exist in scalability and latency. Meanwhile, the FL allows collaborative training of models without compromising the security of the data. Hence, the integrated approach is preferred for application in smart agriculture for the optimization of resources and in smart grids for the secure handling of energy data and optimization of grid operations. Further, the survey looks into the other emerging applications such as autonomous vehicles, Internet of Things (IoT) networks, and industrial automation. Despite all these potentials, there are critical challenges that persist, such as real-time processing, system scalability, and model synchronization. This survey brings to light detailed examinations of existing methods, draws up a list of merits and demerits associated with every application and has undertaken comparative surveys in an assessment of effectiveness as an innovative measure using the blockchain-enabled FL. Finally, future research directions are proposed to address the limitations and enhance the applicability of these technologies in emerging applications.

Keywords

blockchain, federated learning, data security, IoT integration, privacy-preserving computing

I. Introduction

The significance of data is widely embraced, leading to the boom of cloud computing, big data, and Internet of things (IoT) globally. The more the influence of data worldwide, the more will be the issues arising from data security and privacy [1]. For instance, a data breach occurred in Yahoo that put 3 billion users at risk, which is almost half the people of the world [2]. Similarly, many data breaches are happening worldwide, even electronic medical record (EMR)

data, especially protected health information (PHI), is susceptible to privacy risks. In the health care sector, ensuring the privacy of patient records is crucial due to the digitization of records that are vulnerable to cyber threats. Hence, providing safeguards to the sensitive health information of the patients is a basic right for maintaining trust in the organization. However, challenges arise in providing security against unauthorized access to medical records that leads to data stealing, financial scams, misusing

data, etc. It occurs due to the increase in huge data at a rapid speed and cross-institutional data interoperability [3].

Data privacy is enhanced by traditional methods, such as cryptography, access control systems, anonymization, differential privacy, and audit logs. Cryptographic techniques ensure the confidentiality and integrity of data using encryption and homomorphic encryption, though vulnerable to meta-data analysis [4]. Meanwhile, anonymization and pseudonymization assist in hiding and protecting distinct identities in Internet of Things (IoT) data streams, which include static and dynamic techniques. Despite the potential, the technique risks re-identification. Furthermore, access control has the authority to control users in accessing the data and the data itself. It is accomplished using authentication mechanisms, authorization policies, and user permissions, while restricted by centralization. Furthermore, differential privacy merges random noise with probe reactions to protect user data confidentiality, which is not influenced by user appearance or query results. The privacy budget is estimated to affirm a mathematically strong privacy; however, utility balance is interrupted in health data [5, 6].

In recent years, multiple trends have been integrated for privacy preservation, such as integrating Artificial Intelligence (AI), which is a dynamic, progressing field, particularly in IoT-based cloud systems. Machine learning techniques, such as Random Forest (RF), support vector machines, gradient boosting machines, and logistic regression, are integrated to enhance data anonymization. For instance, AI is used along with homomorphic encryption, adaptive access control systems, etc. Despite their effectiveness, these methods still suffer from potential inaccuracies, inherent biases, and implementation challenges [7, 8]. Similarly, federated learning (FL) is essentially a decentralized paradigm of machine learning that trains across multiple devices without raw data sharing, thus keeping confidentiality and security intact. Though the FL ensures data confidentiality, several challenges persist, such as efficient data management, model convergence, and vulnerability of data transmission [9, 10].

Moreover, the immutable and transparent nature of blockchain enables mitigating some of these issues, but its integration introduces challenges in computational, scalability, and interoperability challenges. Hence, a wide attention has been drawn toward this intersection of blockchain technology with FL. A promising application of the integrated approach is in health care, where patient data privacy holds utmost

importance, and the blockchain ensures secure data without compromising patient confidentiality. However, heterogeneous data sources are required from medical devices, wearables, and electronic health records. Similarly, the privacy and security of urban data, such as traffic patterns, environmental monitoring, and public safety, are provided in smart cities, but the task of providing them is very complex. Furthermore, in smart agriculture, ensuring the secure transmission and privacy preservation of agricultural data, such as crop health, soil moisture, and weather conditions, remains a significant challenge. Nevertheless, heterogeneity in different regions' data and high energy consumption in the agriculture domain affect the generalizability. Further, the integration in smart grid systems have issues in real-time processing in large-scale deployments and also in secure communication between distributed nodes [11, 12].

Moreover, the other emerging applications are in autonomous vehicles, financial systems, construction sectors, and even IoT devices. The former requires secure data transmission within a decentralized fleet of vehicles that precipitated the adoption of blockchain for trust management. With financial systems, fraud detection is enhanced with confidential sensitive financial data. While in edge devices, predictive analytics capabilities are improved in smart homes and for health monitoring systems, challenges still exist in a very high throughput requirement for real-time decision, managing distributed trust over large, highly heterogeneous networks [13–15]. Furthermore, the construction sector uses blockchain's secure, immutable record for managing data and models, while FL ensures privacy. Particularly, the blockchain-enabled smart contracts (BSCs) assure trust, transparency, and data management for efficient monitoring of construction projects to increase efficiency. Meanwhile, the smart contracts assure a secure and transparent platform for all the stakeholders involved [16, 17]. Moreover, integrating blockchain with FL in these domains requires answering questions about consensus mechanisms, latency, and resource limitations of edge devices. The goal is to provide a comprehensive overview of current methods, identify key challenges, and suggest future research directions to enhance the performance and scalability of these technologies.

a. Main contributions of this survey paper

- This paper gives a deep exploration into blockchain-enabled FL across various domains, from health care to smart cities and agriculture, with

emerging applications in autonomous vehicles and even financial systems.

- This work identifies key challenges that lie in the integration of blockchain with FL in terms of scalability, security, computational efficiency, and decentralized trust management. This work also proposes several directions for future research.

b. Structure of the survey paper

The above-mentioned objectives are covered, and various techniques of blockchain integrated FL in various applications have been discussed in the study. The arrangement of this study is as follows: Section II takes five directions about the survey and its objective that are summarized into its ideologies; Section III provides a comparison study; Section IV deals with summarizing the entire survey; Section V

concludes this study; Finally, Section VI deals with a future scope.

II. Literature Survey

In this section, the survey has been provided with discussing blockchain-based secure FL for privacy-preserving in various applications. The method of surveying the various techniques used in different types of fields has been shown in Figure 1.

The survey explores the use of blockchain-Integrated FL in five distinct areas: health care, smart cities, smart agriculture, smart grids, and other applications. These domains are chosen based on substantial body of blockchain-FL research, availability of simulation results, and high practical relevance for data privacy and decentralized analytic requirements, which are absent in domains like finance or defenses.

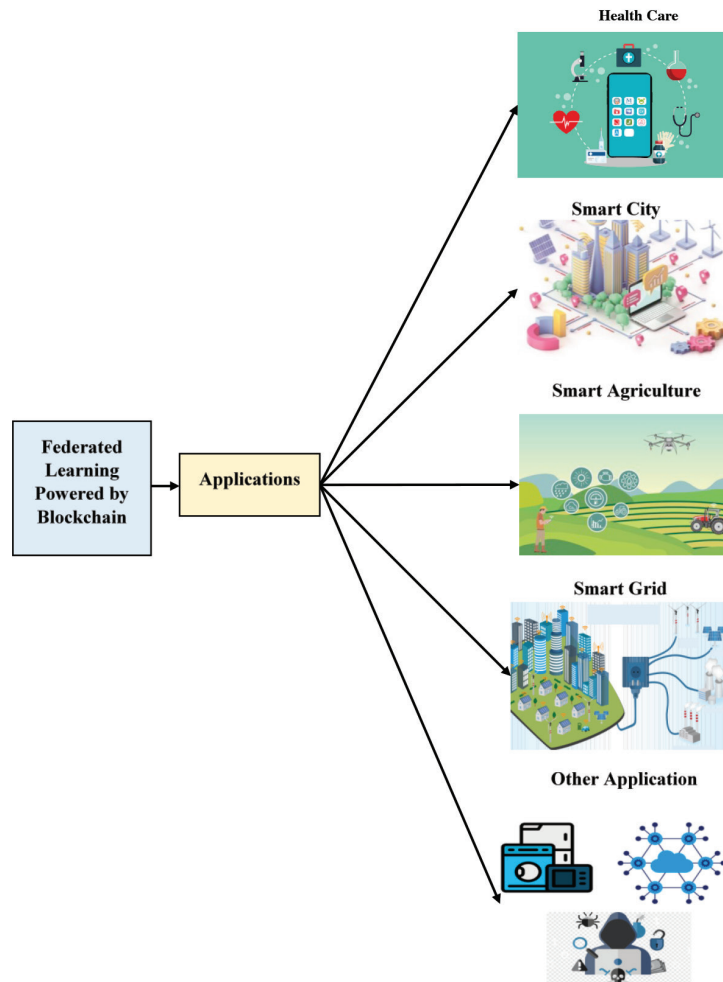


Figure 1: Directions of surveying blockchain integrated FL techniques in various application. FL, federated learning.

a. Survey on blockchain-enabled FL for health care applications

Lakhan et al. [18] proposed a federated learning-enabled blockchain-based task scheduling (FL-BETS) framework that used different kinds of dynamic heuristics. Among these applications are health care applications with hard constraints like deadlines and soft constraints, such as resource energy consumption at the time of execution on distributed fog and cloud nodes. The FL-BETS perspective was identifying and guaranteeing privacy preservation and data fraud prevention at different levels from local fog nodes to remote clouds, all while minimizing energy consumption and delay, and achieving the health care workload deadlines. However, lack of a proper mechanism to enable the study to dynamically adjust to unforeseen changes in network topology, which arise from difficulty in reconciling dynamic network mobility with static blockchain consensus structures, affecting real-time task allocation, has to be addressed.

Baucas et al. [19] proposed a platform based on FL and private blockchain technology within a Fog Computing with the Internet of Things (fog-IoT) network. These technologies have privacy-preserving features that enable secure data within the network. The distributive nature of the fog-IoT network was used to implement an adaptive network for wearable IoT devices. A testbed was designed to test the capability of the proposed platform to preserve the integrity of a classifier. Experimental results showed that the implementation correctly maintained a patient's privacy and integrity of a predictive service. Nevertheless, it faced a scalability problem due to large volumes of wearable devices from the inherent tension between massive IoT concurrency and blockchain's limited throughput, leading to bottlenecks in processing and communication.

Rahman et al. [20] presented a lightweight hybrid FL framework where the blockchain smart contracts handled the edge training plan, trust management, authentication of federated nodes, and the distribution of the globally or locally trained models. The framework further managed the reputation of edge nodes and the datasets or models they upload. It supported full encryption for datasets, model training, and inference processes. The federated edge nodes performed additive encryption, while the blockchain performed multiplicative encryption to aggregate the updated model parameters. The framework was tested using a few Deep Learning (DL) applications designed for clinical trials with COVID-19 patients. However, blockchain finality times inherently lags

behind FL's rapid aggregation cycles, thus causing latency in model aggregation cycles required for efficient FL, creating a lag that disrupts training.

Alshudukhi et al. [21] designed a framework that combined FL with blockchain technology for immediate response to emergencies by utilizing historical patient data. This helped doctors make proper decisions and treat patients individually by summarizing their entire medical history to produce better treatment results. Using both technologies together ensured access to the required information while ensuring the high security of the data with good data privacy. However, the architecture didn't address the trade-off between real-time responsiveness and computational overhead of blockchain verification well, since blockchain cryptographic validation introduces delays incompatible with emergency health care needs.

Alsamhi et al. [22] have been pioneers in the conceptual framework and technical synergy of FL and blockchain for decentralized data sharing to balance the utility and privacy of data. FL, a decentralized machine learning paradigm, enables collaborative AI model training across multiple health care institutions without the sharing of raw patient data. It forms an ecosystem of trust, security, and data integrity when integrated with blockchain. The article was able to explicate the technical underpinnings of FL and blockchain and untangle their roles in revolutionizing health care data sharing, while illustrating the possible implications that this amalgamation can have on patient care. The framework, however, faced problems when it had to handle different data formats and incompatible blockchain frameworks at the institutions, thereby restricting the system's interoperability.

Waheed et al. [23] introduced a new hybrid approach using FL and blockchain technology for IoT-enabled health care applications with secured and privacy-preserved solutions. This approach applied the use of a public-key cryptosystem to provide semantic security in local model updates while preserving integrity through blockchain technology, as well as enforcing access control and accountability. This FL process has enabled a secure model aggregation without sharing the sensitive patient data. Such a framework has been put into practice and tested by using EMNIST datasets, and this framework could effectively preserve the privacy and security of the data while being computationally efficient. However, in such a heterogeneous IoT device capability, FL's synchronous training does not align with the inherently diverse hardware capacities of IoT health care devices, causing imbalanced computational loads, which would degrade system performance.

Ahmed et al. [24] proposed a new method for classifying Artificial Intelligence of Medical Things (AIoMT) devices by the deployment of decentralized processing, known as “Federated Learning”. The approach included the deployment of a system on standard IoT devices and labeled Internet of Medical Things (IoMT) devices for training purposes and attribute extraction. In this manner, interconnected attributes were extracted and mapped from a global federated cum aggregation server. The methodology targeted the extraction of interdependent devices through FL with data privacy, and it strictly followed the policies of operations. Generic labels were applied to categorize devices sending medical data through normal communication channels. However, scalability was an issue in high diversity environments, due to extreme non-IID health care data that challenges stable global aggregation in FL resulting in misclassification.

Ganapathy et al. [25] presented the Block chain enabled Federated Learning for healthcare IoT (BFL-hIoT) model to ensure privacy while training deep learning models that deal with health care data in the health care IoT domain. Here, the data remained decentralized, while the global model was communicated for training by clients through a central server (CS). The proposed model aimed to strike a balance between the demand for privacy and the desire for better performance in machine learning in health care IoT. This study represented the proposed framework BFL-hIoT as a multi-class classifier that would be useful to differentiate between normal and anomalous users by labeling users through target class labels during a class classification of user data records. However, this scheme presents enormous communication overheads both to the clients and CSs, especially in low bandwidth scenarios as FL and blockchain depend on repeated, bandwidth-intensive parameter exchanges.

Ali et al. [26] suggested a blockchain-enabled FL framework along with EMRs as a novel approach that unlocks revolutionary insights into precision medicine. Blockchain-based immutability, transparency, and cryptographic protocols facilitated the conducting of FL on the distributed EMR datasets without patient privacy compromise. Integration of blockchain technology ensured data integrity, traceability, and consent management, thereby alleviating key concerns related to data privacy and security. Through the FL paradigm, machine learning models were trained collaboratively without the need for centralizing EMR data by health care institutions and research organizations. However, high computational and energy costs arose as a result of relying on blockchain, with inherently heavy cryptographic operations and

FL training cycles, which are much less practical for resource-constrained environments.

Kumar et al. [27] used the integration of Permissioned Blockchain and smart contracts along with Deep Learning techniques for developing a novel data-sharing framework, named integration of Permissioned Blockchain and Deep Learning (PBDL) for data-sharing. In detail, the scheme of blockchain has been utilized in the system by registering, verifying via zero-knowledge proof, and validating the entities engaged in the communication process via consensus mechanisms. Authenticated data was then used to suggest a new DL scheme that integrated stacked sparse variational autoencoder (SSVAE) with a self-attention-based bidirectional long short-term memory (SA-BiLSTM). In this scheme, SSVAE encoded health care data into a new format, and SA-BiLSTM enhanced the attack detection process. However, the complexity of the proposed deep learning models significantly increased training and inference times, which hinder real-time application.

The Table 1 summarizes some of the frameworks that have integrated FL with blockchain for health care and IoT applications. Techniques, such as FL-BETS, hybrid FL-blockchain, and BFL-hIoT, maintain privacy, security, and decentralized data sharing while mitigating challenges such as real-time task allocation and model synchronization. Several frameworks emphasize achieving a balance between privacy and performance, for example, adaptive IoT networks and emergency response systems. Lightweight encryption and smart contracts enhance trust, authentication, and efficiency. Challenges include scalability, computational overhead, diversified data formats, and latency in model aggregation. For example, PBDL uses more advanced deep learning models but leads to increased complexity and thus hinders its real-time usage. Moreover, heterogeneous devices have also been an issue due to energy efficiency and imbalanced workloads. Most of these issues arise from inherent architectural constraints that induced synchronization delays and latency, while the protocols in blockchain introduce delays to maintain immutability and trust. These design complexities are required to be addressed to determine the limitations that continuously exist. Overall, they are very advanced frameworks but need optimization before usage.

b. Survey on FL for smart cities with blockchain security

Hai et al. [28] proposed a novel and innovative blockchain-assisted FL approach to secure data sharing in

Table 1: Blockchain-powered FL survey for medical uses

Ref No	Techniques used	Significance	Drawbacks
Lakhan et al. [18]	FL-BETS framework using FL and blockchain, dynamic heuristics	Privacy preservation, fraud prevention, minimized energy consumption, delay reduction, and meeting health care workload deadlines in distributed fog and cloud nodes	No mechanism for dynamically adjusting to unforeseen changes in network topology affecting real-time task allocation
Baucas et al. [19]	FL, private blockchain, adaptive network for wearable IoT devices	Ensures privacy and integrity of classifiers; secures data within fog-IoT networks	Scalability issues with large volumes of wearable devices causing bottlenecks in processing and communication
Rahman et al. [20]	Lightweight hybrid FL framework, smart contracts, additive and multiplicative encryption	Handles training plans, trust management, authentication, reputation tracking, and encryption for privacy; effective in clinical trials for COVID-19	Lacks efficient synchronization for high-frequency updates, causing latency in model aggregation
Alshudukhi et al. [21]	FL, blockchain for emergency response based on historical patient data	Improves treatment results by summarizing medical history, ensures data security and privacy	Poor trade-off handling between real-time responsiveness and computational overhead of blockchain verification
Alsamhi et al. [22]	Conceptual FL-blockchain framework for decentralized health care data sharing	Balances utility and privacy; builds trust, security, and data integrity in collaborative AI model training across health care institutions	Struggles with handling different data formats, restricting system interoperability
Waheed et al. [23]	Hybrid FL-blockchain approach with public-key cryptosystem and access control	Provides secure and privacy-preserved solutions for IoT-enabled health care; computationally efficient	Imbalanced computational loads in heterogeneous IoT devices degrade system performance
Ahmed et al. [24]	FL for classifying AIoMT devices, decentralized processing	Maintains data privacy and extracts interconnected device attributes; applies generic labels to categorize devices in communication	Prone to errors in high-diversity environments; scalability issues
Ganapathy et al. [25]	BFL-hIoT model for decentralized deep learning in health care IoT	Balances privacy demands and performance; multi-class classification of user data records differentiates normal and anomalous users	Communication overheads in low bandwidth scenarios affect clients and CSs
Ali et al. [26]	Blockchain-enabled FL framework with EMRs	Ensures immutability, traceability, and consent management; trains ML models collaboratively without centralizing EMR data	Significant computational and energy costs make it less practical for resource-constrained environments
Kumar et al. [27]	PBDL framework using permissioned blockchain, smart contracts, SSVAE, SA-BiLSTM	Secures data sharing, enhances attack detection through SA-BiLSTM, and converts health care data with SSVAE for better analysis	Complexity of DL models increases training and inference times, hindering real-time application

CS, central server; EMR, electronic medical record; FL, federated learning; FL-BETS, federated learning-enabled blockchain-based task scheduling; IoT, internet of things; PBDL, pyramidal deep-broad learning; SA-BiLSTM, self-attention-based bidirectional long short-term memory; SSVAE, stacked sparse variational autoencoder.

IoT Smart Cities. The process of FL was implemented in a distributed way, and blockchain enhanced the security and resilience of applications in smart cities. Through security analysis, it could be seen that the suggested approach offered comparatively better performance and remained more resistant against various security threats and vulnerabilities. The aggregation model was designed in a decentralized manner to minimize the emerging security risks of the smart city environment. However, the system was demanding significant computational resources for blockchain operations because the decentralized consensus and large-scale FL inherently scale poorly with thousands of smart-city devices, which might deter its deployment in resource-constrained IoT devices.

Abbas et al. [29] proposed an accumulative reputation-based selection (ARS) for edge-aided Unmanned aerial vehicle (UAV) networks based on a differentially private FL framework. The framework used blockchains to prevent single-point failures through the transition from centralized to decentralized control and off-chain model storage using the interplanetary file system (IPFS) with hash-keys maintained on-chain for model integrity. It reduced blockchain size due to the adoption of IPFS and local differential privacy mechanisms that prevent the leakages of privacy. Based on the ARS score, an aggregator is selected and the validators carry out the verification of model. But ARS-based aggregator selection mechanism introduced latency due to the inability of block chain to meet the rapid coordination required in UAV networks hindering the real-time operations.

Guo et al. [30] introduced a data-sharing mechanism integrating blockchain with FL for smart cities. The blockchain ensured credibility of work nodes' performance information and developed a work node selection algorithm and a consensus incentive mechanism namely IPoQ to efficiently support FL tasks. Differential privacy technology was adopted to defend against differential attacks, and experimental results indicated the effectiveness of the proposed data-sharing mechanism. However, the IPoQ incentive mechanism is based on several predefined parameters since the blockchain consensus delays prevent real-time parameter tuning in dynamic urban environments, which lead to sub-optimal consensus performance in dynamic environments of a smart city.

Qolomany et al. [31] presented a Particle Swarm Optimization (PSO)-based method to optimize hyperparameter settings of local machine learning models

within the FL paradigm. The two case studies demonstrated the effectiveness of the proposed technique: one for smart city services on traffic prediction, based on an experimental transportation dataset, and the other for Industrial IoT services, with real-time telemetry dataset-based predictions for machine failures. Experiments indicated that PSO was an efficient approach in tuning the hyperparameters of deep long short-term memory (LSTM) models compared to the grid search method. However, the PSO-based optimization framework suffered from convergence problems for very complex for high-dimensional search spaces especially under decentralized constraints and, thus, gave very inconsistent results.

Kumar et al. [32] proposed a trustworthy privacy-preserving secured framework (TP2SF) for smart cities, which consist of three modules: a trustworthiness module, a two-level privacy module, and an intrusion detection module. The trustworthiness module used a blockchain-based address reputation system. The two-level privacy module made use of a blockchain-enhanced proof of work (ePoW) technique along with principal component analysis (PCA) to transform data so that inference and poisoning attacks can be prevented. The intrusion detection module used an optimized gradient tree boosting system, eXtreme Gradient Boosting (XGBoost). A blockchain-IPFS-integrated Fog-Cloud infrastructure, called CloudBlock and FogBlock, was used to deploy the TP2SF framework in smart cities. However, the two-level privacy module introduced significant processing delays during PCA transformations and ePoW computations, which are computationally intensive, thereby reducing system responsiveness in time-critical applications.

Abdel-Basset et al. [33] proposed Blockchain-based FL framework for pandemic disease diagnosis (BFLPD), which utilized the decentralized nature of blockchain technology to design collaborative intelligence for automated diagnosis without violating trustworthiness metrics, such as privacy, security, and data sharing challenges prevalent in health care systems of smart cities. The CKKS encryption was intelligently redesigned in BFLPD to ensure the secure sharing of learning updates during the training process. The proposed BFLPD provided a decentralized, secure aggregation method that protected the integrity of the global model against adversarial attacks, thus improving the overall efficiency and trustworthiness of the system. However, the approach lacked a comprehensive evaluation of scalability when handling a rapidly increasing number of participants in the decentralized network.

Muhammad et al. [34] proposed a Secure and Transparent Traffic Congestion Control System using FL to address the increasing problems of traffic congestion in smart cities. The main issues in the existing traffic congestion control systems included data privacy, security vulnerabilities, and the need for joint decision-making. FL enabled the training of models on decentralized data without compromising data privacy. Moreover, adding blockchain technology enhanced the safety, integrity, and transparency of the system. In the proposed system, FL was used for securely collecting and analyzing the local traffic data from various sources present in a smart city, without moving sensitive data out of its location. There was no adaptive mechanism for handling abrupt traffic anomalies due to unexpected events, such as accidents or emergencies, in real-time response, as FL updates and blockchain confirmations operate on slow periodic cycles.

Yin et al. [35] proposed an efficient attribute-based participant selection scheme to allow only those individuals who were eligible for the task publisher to participate in training while maintaining high privacy requirements. This improved efficiency and defended against attacks. The scheme was further extended to incentivize clients to participate in FL and to provide an audit mechanism by using a consortium blockchain. An in-depth comparison of the scheme to other schemes was presented. The evaluation results revealed that the scheme improved FL's efficiency in making reliable participant selection possible, thus increasing the usage of FL in smart cities. However, it failed to address the biased potential due to the inherent statistical distortions caused by privacy-driven selective sampling in FL, in which the restricted participant selection criteria were introduced. This reduction in the model's generalizability made it undesirable.

Padma et al. [36] proposed a new blockchain-based framework for the security and integrity concerns of IoT data. The framework, called SecPrivPreserve, secured its phases: initialization, registration, data protection, authentication, data access control, validation, and data sharing and download. Various mechanisms, such as One Time Passwords (OTP), encryption, and hashing, were used at different stages to enhance confidentiality, privacy, and integrity. Since the SecPrivPreserve framework was tested on a permissioned blockchain platform, tamper-proofing and non-repudiation were automatically considered. Besides, data protection used Chebyshev polynomials and interpolation. The framework was experimented with and deployed using Fabric SDK. However, the framework's reliance on permissioned blockchain

limited interoperability with other blockchain systems, as blockchains lack universal standards for identity and cross-chain communication, which could be an obstacle to its wider use in diverse IoT environments.

Far et al. [37] carried out research on the blockchain and deep reinforcement learning (DRL) integration toward optimizing mobile transmission and safe data exchange in IoT-supported smart cities. The combination of DRL and blockchain was shown to improve the performance of IoT networks by maintaining privacy and security through clustering and categorization of IoT application systems. By combining blockchain's decentralized framework with DRL, the investigation showed how this approach addressed privacy and security issues, improved mobile transmission efficiency, and guaranteed robust, privacy-preserving IoT systems. Moreover, blockchain integration for DRL and notable applications of DRL technology were investigated. However, the approach lacks any rigorous analysis of energy consumption in resource-constrained IoT devices when deploying DRL and blockchain integration, which are inherently power-intensive processes, impacting system efficiency.

The Table 2 depicts some blockchain-FL methods that have been used to tackle privacy, security, and efficiency in smart cities and IoT environments. Decentralized control, IPFS for model integrity, differential privacy, and encryption were some of the techniques used to enhance system resilience against threats. Optimization methods like PSO improved model performance, while frameworks like TP2SF and SecPrivPreserve ensured privacy and intrusion detection. Applications included traffic congestion control, automated diagnosis, and efficient participant selection, which were showing improved data sharing and decision making. However, the problems of high computational demands, latency in real-time operations, scalability issues, and energy inefficiency in resource-constrained devices remain significant obstacles to wide-scale adoption and efficiency. These challenges arise from the properties of the system, where the blockchain integration induces latency in most decentralized smart-city deployments, while ensuring security. Similarly, FL scalability issues occur due to heterogeneous devices, non-IID data, and frequent communication iterations, which are intrinsic to real-world IoT environments.

c. Survey on blockchain-based FL in smart agriculture

Shen et al. [38] presented a Blockchain-Assisted Federated Learning (BAFL) driven Support vector

Table 2: Survey on FL for blockchain-securized smart cities

Ref No	Techniques used	Significance	Drawbacks
Hai et al. [28]	Blockchain-assisted FL for IoT smart cities	Enhanced security, resilience, and performance in smart city applications	High computational demands for blockchain operations, unsuitable for resource-constrained IoT devices
Abbas et al. [29]	ARS with IPFS and FL for UAV networks	Decentralized control, model integrity through IPFS, and privacy preservation	Latency introduced by ARS-based aggregator selection hindered real-time UAV operations
Guo et al. [30]	Blockchain-integrated FL with work node selection and IPoQ incentive mechanism	Credibility of node performance, efficient FL tasks, and defense against differential attacks	Predefined parameters in IPoQ lead to suboptimal performance in dynamic environments
Qolomany et al. [31]	PSO-based hyperparameter optimization for FL in smart cities and IIoT	Effective hyperparameter tuning for traffic prediction and machine failure predictions	Inconsistent results in complex or high-dimensional search spaces due to convergence issues
Kumar et al. [32]	TP2SF with blockchain and PCA	Enhanced privacy, security, and intrusion detection for smart cities	Significant processing delays from PCA transformations and ePoW computations, reducing responsiveness in time-critical applications
Abdel-Basset et al. [33]	Blockchain-FL with CKKS encryption (BFLPD) for automated diagnosis in smart cities	Secure and trustworthy aggregation, protection against adversarial attacks, and improved system efficiency	Limited scalability evaluation when handling an increasing number of decentralized participants
Muhammad et al. [34]	FL with blockchain for traffic congestion control	Secure, privacy-preserving traffic data analysis with improved safety, integrity, and transparency	No adaptive mechanism for handling real-time traffic anomalies due to emergencies or accidents
Yin et al. [35]	Attribute-based participant selection with consortium blockchain for FL	Efficient, reliable participant selection and incentivized client participation in smart city FL applications	Biased participant selection reduced the model's generalizability
Padma et al. [36]	SecPrivPreserve framework with permissioned blockchain for IoT	Enhanced confidentiality, privacy, and integrity with tamper-proofing and non-repudiation	Limited interoperability with other blockchain systems, restricting wider use
Far et al. [37]	Blockchain and DRL integration for IoT in smart cities	Privacy-preserving and efficient mobile transmission with improved IoT network performance	Lack of rigorous energy consumption analysis for resource-constrained IoT devices, impacting system efficiency

ARS, accumulative reputation-based selection; DRL, deep reinforcement learning; ePoW, enhanced proof of work; FL, federated learning; IoT, internet of things; IPFS, interplanetary file system; TP2SF, trustworthy privacy-preserving secured framework.

Machine (SVM) framework to accomplish efficient data sharing and privacy protection. BAFL-SVM was composed of FedSVM-RiceCare module and FedPrivChain module. Specifically, the model in FedSVM-RiceCare was trained by using FL and SVM

to enhance experimental accuracy. In FedPrivChain, homomorphic encryption and a secret-sharing scheme were used to encrypt the local model parameters before uploading. Extensive experiments on a real-world dataset of rice pests and diseases were

conducted, and the experimental results showed that the framework not only ensured secure data sharing but also achieved higher recognition accuracy compared to other schemes. But this structure needed much computation to carry out encryption and decryption, due to the requirement of significant processing, which make them unsuitable for low-power or resource-constrained devices.

Praharaj et al. [39] presented a multi-layered architecture with DT to emphasize the security challenges in cooperative smart farming. They further proposed a hierarchical federated transfer learning framework to handle and mitigate security threats against collaborative smart farming. In this approach, FL-based anomaly detection (AD) was used, running on edge servers, and allowed AD models to run locally without exposing farm data. This localization had outstanding generalization ability and greatly increased the detection of unknown cyber-attacks. A hierarchical FL structure was used, where aggregation support at various levels was supported to foster multi-party collaboration. Furthermore, the approach had the essence of Convolutional Neural Networks (CNNs) and LSTM models, which was further enhanced through transfer learning. However, the hierarchical structure caused much latency and communication overhead, while multi-level aggregation introduced unavoidable synchronization delays across layers, which negatively impacted anomaly detection in a real-time application.

Singh et al. [40] suggested a new architecture using the combination of blockchain technology and FL in enhancing the security of smart farming systems (SMSs) against external threats. Integrating blockchain technology provides authenticity of data and maintains data storage transparently, and the FL facilitates collaborative training models without compromising data privacy. The architecture utilizes an ensemble layer (EL) to train data from each smart land while maintaining safety along with privacy measures. Each device used FL techniques on smart land to collaboratively train intrusion detection models where the confidentiality of sensitive information was maintained. Data was aggregated at the Authentication Layer, and the PoAh Consensus Algorithm was utilized for authenticating data on smart land. However, the use of consensus algorithms led to scalability problems, whose complexity grows with the network size, especially in scenarios with a large number of participating nodes.

Vimalajeewa et al. [41] proposed a novel joint FL model based on Neural Network (NN) and Partial Least Square (PLS) regression (FL-NNPLS). Its predictive performance was evaluated under sequential and

parallel updating-based FL algorithms in the context of smart farming for milk quality analysis. Smart farming is a fast-growing industrial sector requiring effective analytics platforms to enable sustainable farming practices. The FL-NNPLS approach outperformed the centralized approach and showed state-of-the-art performance. Although the NN-based models have various advantages, their use in FL settings was limited by thin clients with low computational capabilities and high-dimensional data with numerous model parameters. However, the model faced difficulties in handling dynamically changing data distributions, which led to inconsistencies in prediction accuracy over time because of distributed clients with heterogeneous capabilities and local data distributions, making consistent model updates fundamentally difficult in decentralized settings.

Leduc et al. [42] focused on the design, development, and application of innovative methods to use modern information and communication technologies, such as the IoT and machine learning, to move toward more sustainable agricultural and farming practices. This paper highlighted that most blockchain-based farming frameworks concentrated on food tracking and traceability. There is scant research done to focus on the design of digital markets to enable trade among farmers and other third-party participants or for conducting performance reviews of the proposed frameworks. However, dependency upon stability and high speed in a network has hampered connectivity in most areas related to rural farming and is mostly not applicable there due to the lack of network reliability as in blockchain and FL.

Hasan et al. [43] proposed a blockchain-based solution that harnessed intrinsic features of this innovative and disruptive technology to tap into transparency, reliability, authenticity, and accountability within an agricultural supply chain. Furthermore, the solution removed misleading food labels on fresh produce by providing consumers with the ability to trace and verify the origin and authenticity of the source of food transparently. The sustainable solutions implemented were clear, and all the standards met were from different sustainable food certifications and agencies, including organic, non-Genetically Modified Organisms (GMO), and Good Agricultural Practices (GAP). The solution failed to scale to larger agricultural ecosystems, which required maintaining transparency and traceability across multiple stakeholders, hence posing integration problems with complex and diverse farming networks.

Chaganti et al. [44] suggested a cloud-enabled smart-farm security monitoring framework for

monitoring the status of devices and sensor anomalies effectively to counter security attacks using behavioral patterns. Further, a blockchain-based smart-contract application was implemented to store the security-anomaly information safely and proactively counter the same attacks on other farms in the community. The security-monitoring-framework prototype for smart farms using Arduino Sensor Kit, ESP32, Amazon Web Services (AWS) cloud, and smart contract on the Ethereum Rinkeby test network monitored and responded to latency within the network. Its disadvantage was that it completely depends on a single service in the cloud, which linked the system with provider's availability and performance. This caused an increased risk of being prone to service outages as well as vendor lock-ins with reduced system robustness.

Kumar et al. [45] presented a secure privacy-preserving framework (SP2F) for smart agricultural UAVs. The SP2F framework had two major engines: a two-level privacy engine and a deep learning-based anomaly detection engine. The two-level privacy engine in the framework comprised a blockchain and smart contract-based ePoW designed for data authentication to prevent data poisoning attacks. A Sparse AutoEncoder or SAE was applied to data, transforming it into a new form, encoded, to hinder inference attacks. Here in the anomaly detection engine, a stacked long short-term memory (SLSTM) was trained on the results of the offered two-level privacy engine, applying them on two publicly available datasets based on IoT, namely, ToN-IoT, and IoT Botnet. However, the energy and computational limits of UAVs make real-time encryption, anomaly detection, and SLSTM processing challenged the framework in handling UAV hardware constraints, which might lead to reduced efficiency in resource-constrained scenarios.

Pranto et al. [46] identified all the various features and opportunities of using blockchain along with smart contracts with the IoT-enabled integration in the pre-harvesting and post-harvesting parts of the agriculture segment. They have proposed a system, based on blockchain as its main infrastructure, with the involvement of IoT devices at field-level data collection and further using smart contracts for regulations across all contributing parties in an interaction. The implementation diagrams for this system were shown with a step-by-step explanation. Costs of gas for all operations were also added in order to provide a clearer vision of costs. However, in multi-party disputes, blockchain's immutability and deterministic smart contracts limit flexibility in resolving nuanced conflicts and, therefore,

has proved less effective in resolving complex contractual disputes in agricultural cases.

Sakthi and DafniRose [47] evaluated the performance of a blockchain-assisted secured smart agriculture system by recording the execution time and communication overhead. Private blockchain services were developed to authenticate users and other devices in the vehicular network, and experiments have been conducted. Blockchain was able to provide authenticity, security, and privacy for the users and other actors in the IoV. Different days in the cloud environment recorded various mobile user query response times. TID was the abbreviation of Transaction Identification Number and denoted the time taken by the cloud service to process the query and send back a response to the internet user. However, central cloud environments raised dependency-related issues of single points of failure and potential performance bottlenecks. The dependency on a central cloud for blockchain authentication is a structural issue.

Table 3 presents exciting new applications of blockchain, FL, IoT, and advanced algorithms to smart agriculture. Techniques used, such as FL-SVM and hierarchical federated transfer learning, improved data security accuracy and anomaly detection, but suffer from high computational demands as well as latency. However, with the integration of blockchain with FL and IoT, it had issues with scalability and resolution of multi-party conflict; with advanced models such as FL-NNPLS and SP2F, the state-of-the-art anomaly detection and data protection came into existence, with limitations in handling dynamic data and resource-constrained environments. The studies notwithstanding, the contributions underscore dependence on stable networks and centralized systems, which significantly increases the risks for rural or large-scale applications. Most of these limitations are due to inherent technological principles, since, the cryptographic operations of blockchain and iterative updates of FL are naturally resource-intensive, which increases the computational costs. Additionally, integration of decentralized learning in rural, bandwidth-limited agricultural settings induces consensus delays and communication overhead.

d. Survey on securing smart grid (SG) data through blockchain-driven FL

Ashraf et al. [48] proposed a new FL framework, FedDP, to address energy theft detection. This framework allowed different clients to experience on-device prediction with reduced communication

Table 3: Blockchain-based FL survey for smart agriculture

Ref No	Techniques used	Significance	Drawbacks
Shen et al. [38]	Blockchain-assisted FL with SVM, homomorphic encryption, secret sharing	Ensures secure data sharing and achieves higher recognition accuracy for rice pest and disease detection	High computational requirements for encryption and decryption, impractical for low-power devices
Praharaj et al. [39]	Multi-layered DT architecture, federated transfer learning, FL-based AD, CNNs, LSTM models	Enhances security and detects unknown cyber-attacks effectively in smart farming	High latency and communication overhead, negatively impacting real-time anomaly detection
Singh et al. [40]	Blockchain with FL, EL, PoAh consensus algorithm	Maintains data authenticity, privacy, and collaborative training for intrusion detection in SMSs	Scalability challenges with a large number of nodes due to consensus algorithms
Vimalajeewa et al. [41]	Joint FL model (FL-NNPLS) with NN and PLS regression	Outperforms centralized models, achieving state-of-the-art results in milk quality analysis	Difficulty handling dynamic data distributions, inconsistencies in prediction accuracy
Leduc et al. [42]	IoT and ML-based modern ICT applications	Supports sustainable agricultural practices, emphasizing food tracking and traceability	Dependency on stable high-speed networks limits rural farming applicability
Hasan et al. [43]	Blockchain-based transparent supply chain solutions	Enhances food source authenticity and reliability, meets various sustainability standards	Poor scalability for larger ecosystems, integration challenges in diverse networks
Chaganti et al. [44]	Cloud-enabled security monitoring, blockchain-based smart contracts	Effectively monitors security anomalies and proactively counters attacks in community farms	Single cloud service dependency risks outages and reduces robustness
Kumar et al. [45]	SP2F with ePoW, smart contracts, SAE, SLSTM	Prevents data poisoning attacks and enhances anomaly detection in UAV-enabled agriculture	Limited efficiency in resource-constrained UAVs due to hardware constraints
Pranto et al. [46]	Blockchain with IoT integration and smart contracts	Provides stepwise clarity for cost management in pre- and post-harvesting	Less effective in resolving complex multi-party contractual disputes
Sakthi and DafniRose [47]	Blockchain-assisted smart agriculture with private blockchain services	Ensures authenticity, security, and privacy in the IoV	Centralized cloud dependency introduces point of failure risks

AD, anomaly detection; EL, ensemble layer; FL, federated learning; ICT, information and communication technologies; IoT, internet of things; IoV, internet of vehicles; LSTM, long short-term memory; SAE, sparse autoencoder; SP2F, secured privacy-preserving framework; SLSTM, stacked long short term memory.

overhead while learning from the experiences of other clients through a CS. In addition to the above, a federated voting classifier (FVC) was proposed using novel majority voting-based consensus by traditional machine learning classifiers, including RFs, k-nearest neighbors, and bagging classifiers for the accurate detection of energy theft. Based on their knowledge, these classical ML classifiers had never been applied

in a federated way for the detection of energy theft in SGs. However, the design was scalable and had scalability issues while integrating a large number of heterogeneous clients with varied computational resources, as FL inherently requires synchronization across devices with different capabilities.

Zhang et al. [49] introduced a privacy protection scheme for smart meters in decentralized smart

home environments based on a consortium blockchain. The scheme mitigated the security issues that included single point failure and malicious data tampering with the use of elliptic curve point multiplication in a certificateless aggregated ring signcryption algorithm, which was reduced to computing and communication costs. A consortium blockchain was used for the distributed storage of user data to eliminate issues of single-point failure and data tampering. Theoretical analysis showed that the scheme ensures user privacy with confidentiality and unforgeability, whereas experiments reveal decreased computing and communication costs. However, the method was not found to work effectively in achieving interoperability among various blockchain frameworks and legacy smart grid infrastructures due to its heterogeneous nature, which is difficult to standardize.

Yilmaz et al. [50] handled the privacy violation of energy usage data acquired from the smart meters. They come up with a new novel solution to support the prevention of privacy along with supporting the analytics on energy data. They experimented the implementation of occupancy detection attacks, using a deep neural network, with promising high-accuracy results. The introduced framework is termed as adversarial machine learning occupancy detection avoidance-B (AMLODA-B). This framework employed a LSTM model within the smart metering infrastructure to prevent leakage of personal information. However, the reliance on deep learning models increased the computational load, which was intrinsic to LSTM-based privacy preservation on resource-constrained smart meters.

Fan et al. [51] presented a decentralized privacy-preserving data aggregation scheme for the smart grid through blockchain. They applied the leader election algorithm for the selection of the best mining node in the residential zone, which acts as a mining node that constructs the block. A node, within this framework, employed an algorithm from the Paillier cryptosystem for power consumption data aggregation; they used the Boneh-Lynn-Shacham (BLS) short signature along with SHA 256 function for privacy in the aggregation process and assurance of data integrity, respectively. This scheme protected the privacy of users while achieving decentralization, eliminating the requirement for Trusted Third Party (TTP) or Certificate Authority (CA). Security analysis showed that the scheme satisfied the privacy and security requirements for smart grid data aggregation. However, the dependency on leader election algorithms led to uneven load distribution and increased

latency under heavy network traffic conditions, which was an inherent limitation of decentralized mining-based aggregation schemes.

Lu et al. [52] suggested a light weight Edge blockchain -assisted Data Aggregation scheme (EBDA) for preserving privacy for the smart grid. The architecture applied edge computing and blockchain across a three-layered model that supported a two-tier data aggregation model with a significant increase in efficiency as well as security. In theoretical analysis and simulation, they showed that EBDA has strong resistance to network attacks with lower computation cost and also reduces communication overhead than earlier schemes. However, with edge blockchain adoption, synchronization became a problem between the different edge nodes, especially in high-frequency updates, because coordinating frequent updates across distributed nodes inherently introduces delays.

Jithish et al. [53] proposed an FL-based anomaly detection scheme for smart grid in which ML models have been trained locally on a smart meter without sharing with a CS, keeping the user's privacy into consideration. In the new approach, a global model was downloaded from the server at the smart meters for on-device training. After local training, the local model parameters are sent to the server with the intention of improving the global model. Model parameter updates were secured from the adversaries using the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol. Using the standard datasets, they experimentally probed the performance of anomaly detection in FL and found that FL models could attain the same level of anomaly detection performance as centralized ML models but without compromising users' privacy. However, this reliance on SSL/TLS did not fully address adversarial poisoning of parameter updates during aggregation, because securing parameter transmission alone failed to address malicious updates in FL, which was a fundamental limitation of current aggregation methods.

Su et al. [54] presented a secure FL-enabled Artificial Intelligence of Things (AIoT) scheme for private energy data sharing in smart grids with edge-cloud collaboration. Specifically, the authors proposed an edge-cloud-assisted FL framework for communication-efficient and privacy-preserving energy data sharing of users in smart grids. Based on the consideration of non-IID effects, they presented a local data evaluation mechanism in FL and formulated two optimization problems for Energy Data Owners (EDOs) and ESPs. Because the knowledge of multi-dimensional user private information is very scarce in practical scenarios, they proposed a two-layer deep

reinforcement learning-based incentive algorithm to encourage EDOs' participation and high-quality model contribution. However, this incentive mechanism faced challenges from a scalability perspective since incentive mechanisms struggle to handle a tremendous number of users and energy providers, which significantly caused a problem from the computation aspect.

Fekri et al. [55] suggested FL for load forecasting using smart meter data. This approach allowed training a single model on all the participating smart meters without sharing local data. Two alternative FL approaches were tested: FedSGD, which executed one step of gradient descent on clients before aggregating updates on the server, and FedAVG, which executed multiple steps before aggregating. Specifically, residential consumers are heterogeneous, and therefore, it is difficult to train one model because the load profiles were different for each consumer. The results indicate that Federated Averaging (FedAVG) performed better in terms of accuracy compared to Federated Stochastic Gradient Descent (FedSGD), which also required fewer communication rounds. However, diversity in the consumption patterns of residential often resulted in suboptimal convergence for households whose consumption patterns were unique or extreme, which made a single federated model unable to fit all clients accurately.

Li et al. [56] proposed a false data injection attack (FDIA) detection method based on secure federated deep learning by combining the transformer, FL, and the Paillier cryptosystem. The transformer, as a detector deployed in edge nodes, delved deep into the connection between individual electrical quantities using its multi-head self-attention mechanism. This approach utilized the data of all nodes in a FL framework to collaboratively train a detection model by keeping the data local during training and preserving data privacy. To improve the security of FL, an innovative scheme for secure FL was designed with the combination of the Paillier cryptosystem and FL. However, the computational overhead of the Paillier cryptosystem increased real-time anomaly detection latency much more than expected.

Shrestha et al. [57] proposed an anomaly detection system to detect threats and utilized FL to address issues of data silos and data privacy. The framework identified anomalies in industrial data gathered from remote terminal devices deployed at substations in the smart electric grid system. The anomaly detection system involved LSTM, autoencoders, as well as mean standard deviation and median absolute

deviation approaches to identifying anomalies. To improve the security and privacy properties of the proposed framework, they implemented homomorphic encryption along the lines of the Paillier algorithm. However, the use of homomorphic encryption added considerable computational and energy costs, as the encryption itself is inherently resource-intensive in privacy-preserving anomaly detection, which were impractical for edge devices with limited resources.

Table 4 summarizes several privacy-preserving and anomaly detection techniques for smart grids. Many of these research studies have been conducted focusing on FL, consortium blockchain, and edge computing to address the above issues such as energy theft detection, privacy protection, and false data injection attacks. FL provides a decentralized solution, allowing local model training to protect user privacy. Scalability and computational load are big concerns, especially for devices with limited resources. Data tampering on blockchain and elliptic curve-based cryptosystems mitigates, but the difficulty remains in interoperability with legacy systems. Another, deep learning methods of LSTM and autoencoders suffer from computational load; these cannot be used directly at the edge device level due to computational intensity. In summary, the techniques are enhancing security, privacy, and efficiency, but require further optimization in terms of scalability and computational demands. These drawbacks are attributed to fundamental system constraints, such that decentralized architectures induce consensus latency, cryptographic overhead, and leader election delays. Similarly, FL struggles with heterogeneous clients and high-frequency data in the distributed learning systems design.

e. Survey on blockchain-based FL for other emerging applications

Zhao et al. [58] proposed a FL system, which incorporated a reputation mechanism to aid home appliance manufacturers in machine learning model training based on customers' data. The use of this system enabled the manufacturers to predict customers' requirements and consumption behaviors. The workflow of the system consisted of two stages. In the first stage, customers used mobile phones and Mobile Edge Computing (MEC) servers to train an initial model offered by the manufacturer. The clients started to collect data of these domestic appliances from their phones; they then downloaded the initial models, which then gave them the required training locally on these sets. Once they obtained

Table 4: Survey on using blockchain-powered FL to secure smart grid data

Ref No	Techniques used	Significance	Drawbacks
Ashraf et al. [48]	FL (FedDP), FVC, RF, KNN, BG	Addresses energy theft detection with reduced communication overhead and energy-efficient on-device prediction	Scalability issues when integrating heterogeneous clients with varied computational resources
Zhang et al. [49]	Consortium blockchain, certificateless aggregated ring signcryption	Enhances privacy protection for smart meters by eliminating single points of failure and data tampering	Issues with interoperability among blockchain frameworks and legacy systems
Yilmaz et al. [50]	Adversarial machine learning, LSTM, blockchain	Protects energy usage data from privacy violations while supporting analytics on energy data	Increased computational load due to deep learning reliance, unsuitable for resource-constrained smart meters
Fan et al. [51]	Leader election algorithm, Paillier cryptosystem, Boneh-Lynn-Shacham short signature, SHA 256	Decentralized privacy-preserving data aggregation with a focus on security and privacy for smart grids	Uneven load distribution and increased latency under heavy network traffic
Lu et al. [52]	Edge blockchain, lightweight privacy-preserving aggregation, edge computing	Enhances efficiency and security in smart grids with reduced computation costs and communication overhead	Synchronization issues among edge nodes, particularly during high-frequency updates
Jithish et al. [53]	FL, SSL/TLS protocol	Provides anomaly detection while ensuring user privacy by training models locally on smart meters	Reliance on SSL/TLS, which does not fully protect against adversarial poisoning of parameter updates
Su et al. [54]	FL, Edge-cloud collaboration, deep reinforcement learning	Privacy-preserving energy data sharing with incentives for participants in smart grids	Scalability issues due to a large number of users and energy providers, causing computation challenges
Fekri et al. [55]	FL (FedSGD, FedAVG)	Enables load forecasting on smart meters without sharing local data, improving data privacy	Diversity in consumer load profiles causes suboptimal convergence for some households
Li et al. [56]	Secure federated deep learning, transformer, Paillier cryptosystem	Detects FDIA while preserving privacy and enhancing detection accuracy	Increased real-time detection latency due to the computational overhead of the Paillier cryptosystem
Shrestha et al. [57]	FL, LSTM, autoencoders, homomorphic encryption (Paillier algorithm)	Identifies anomalies in industrial smart grid data while ensuring data privacy	High computational and energy costs are the primary barriers to deploying modern AI models on edge devices with limited resources

BG, bagging classifiers; FDIA, false data injection attacks; FL, federated learning; LSTM, long short-term memory.

their local models, customers started to digitally sign those models and uploaded them on to blockchain. The contribution in global model by those was uniform for all diverse customer quality which caused its possible bias in global models, because FL inherently assumes equal influence, ignoring client data quality heterogeneity.

ur Rehman et al. [59] proposed a new idea of fine-grained FL to decentralize shared ML models on edge servers. They formally extended the definition of the fine-grained FL process in mobile edge computing systems and defined the core requirements of fine-grained FL systems, which include personalization, decentralization, incentive mechanisms, trust, activity

monitoring, heterogeneity, context-awareness, model synchronization, and communication and bandwidth efficiency. In addition, they proposed the concept of blockchain-based reputation-aware fine-grained FL to ensure trustworthy collaborative training in mobile edge computing systems. However, the fine-grained FL approach faced problems with managing high computational overhead during model synchronization, especially in heterogeneous edge environments with diverse client capabilities.

Li et al. [60] presented a decentralized FL framework, based on blockchain and known as the Blockchain-based federated learning framework with committee consensus (BFLC). The framework exploited blockchain for global model storage and local model update exchange. To facilitate BFLC, an innovative committee consensus mechanism was developed, which brought to the fore diminished consensus computation, resulting in reduced malicious attacks. The scalability of BFLC, including theoretical security, storage optimization, and incentives were also discussed. However, the committee-based consensus mechanism was prone to delay model updates for time-sensitive tasks under heavy network traffic, as distributed consensus is inherently slower than centralized aggregation.

Zhang et al. [61] designed a blockchain-based smart agent system architecture and applied it in FL. The FL technique trained models across multiple devices or servers holding private data samples without exchanging the data. Locally the trained results were aggregated by a centralized server in a privacy-preserving way. The proposed smart agent model created a new architecture composed of agents forming a blockchain network. A fully decentralized, privacy-preserving smart agent blockchain-FL framework was proposed where every smart agent acted as a peer of a blockchain network and participant of an FL task. Finally, artificial neural network demonstration was carried out to validate the framework's efficacy. With each increase in the number of smart agents, the complexity of the architecture increased, thereby causing problems in managing and synchronizing the decentralized network, because a fully decentralized FL inherently required coordination among all peers.

Wang et al. [62] designed an autonomous blockchain-empowered privacy-preserving FL framework. Here, mobile edge computing technology was implemented in the Internet of Vehicles (IoV) system. Techniques related to differential privacy were utilized to manage privacy. To ensure honesty of the participants, a malicious updates removal algorithm using a self-reliability filter was designed. Concurrently, the

authors introduced a double aggregation frame to reduce communication overhead while maintaining the quality of the training model. In blockchain, an FL participant management system was developed such that any models uploaded there cannot be changed due to the recording of quality. Nonetheless, the differential privacy techniques have reduced model performance, leading to a trade-off between preservation of privacy and training accuracy.

Qi et al. [63] proposed a consortium blockchain-based FL framework to enable decentralized, reliable, and secure FL without a centralized model coordinator. In the proposed framework, the model updates from the distributed vehicles were verified by miners to prevent unreliable model updates and were then stored on the blockchain. Besides, to further protect model privacy on the blockchain, a differential privacy method with a noise-adding mechanism was applied to the blockchain-based FL framework. Numerical results illustrated that the proposed schemes could effectively prevent data poisoning attacks and improve the privacy protection of model updates for secure and privacy-preserving traffic flow prediction. However, it is noteworthy that relying on miners for verifications can lead to delaying model update processing and impair real-time prediction performance, especially in critical traffic applications, as blockchain consensus and differential privacy inherently introduce latency in time-sensitive traffic applications.

Wang et al. [64] proposed a blockchain-based privacy-preserving FL scheme named BPFL that utilizes blockchain as the underlying distributed framework for FL. The Multi-Krum technology was enhanced, and homomorphic encryption was integrated to achieve ciphertext-level model aggregation and model filtering in order to allow the verification of the local models and still achieve privacy preservation. Moreover, they designed a reputation-based incentive mechanism to guide users in the IoV to actively participate in FL and practice honesty. Through security analysis and performance evaluation, the results indicated that the presented scheme could meet the proposed security requirements and improve the FL model performance. However, the introduction of homomorphic encryption will probably add significant computational overhead that impacts the efficiency of the system in low-resource computational environments in privacy-preserving FL.

Moulahi et al. [65] applied classification approaches to Vehicular Ad Hoc Network (VANET) and intelligent transport systems (ITS) cyber-threat detection at the vehicle level. Then, they used

blockchain and applied an aggregation strategy to different models. The models of the previous step were uploaded into a smart contract, and the updated models were returned to the vehicles. They also conducted an experimental study to measure the effectiveness of the proposed prototype. In this paper, the VeReMi dataset was divided into five parts in a balanced manner for the experimental study. Classification techniques were executed by each vehicle separately, and models were generated. After the aggregation of the models in the blockchain, they were returned to the vehicles. However, model aggregation in the blockchain might be slow as the distributed ledger consensus is inherently time-consuming, which would be a counter to the fast response required in a high-speed vehicle network.

Hua et al. [66] proposed a method on blockchain-based FL to implement asynchronous collaborative machine learning between the distributed agents that owned data. This method performed distributed machine learning without a trusted CS. The blockchain smart contract was used to manage the whole FL process. The FL approach employed a support vector machine-based intelligent control model based on historical driving data retrieved from real heavy haul rail systems. A mixing kernel function that was constructed of polynomial and radial basis functions (RBFs), with the help of a dynamic weight factor varying with train speeds improved model accuracy. However, since SVM is employed, its dependency may have limitations toward scalability in larger complex systems that exist within real rail systems, because traditional kernel-based models do not scale efficiently with large datasets or many agents.

Durga et al. [67] presented a novel framework based on blockchain and the FL model. The FL model addressed reduced complexity, while blockchain helped in maintaining privacy in distributed data. More precisely, the proposed FL ensembled deep learning blockchain model framework collected data from different medical health care centers and developed the model with a hybrid capsule learning network. It made predictions accurately with privacy preservation and sharing, but the complexity of ensemble deep learning models may lead to increased computational requirements and performance issues in resource-constrained health care environments with limited processing power.

Several FL systems, leveraging blockchain, are presented in Table 5, for various applications, ranging from home appliance prediction and medical health care to vehicular networks. These systems exploit decentralized models with privacy-preserving

techniques, such as differential privacy and homomorphic encryption. The blockchain further ensures secure updating of models and participant verification, whereas in some systems, reputation mechanisms promote honest collaboration. However, several challenges are associated with FL, such as high computational overhead during model synchronization, mainly with fine-grained FL and SVM-based models, slow aggregation due to network delays, and trade-offs between privacy and model accuracy. Some of the frameworks face scalability problems, such as complexity in synchronization and computational requirements, especially in resource-constrained environments. These issues persist from fundamental characteristics of blockchain and FL rather than due to implementation flaws, which introduced computational and communication delays. Although these systems have limitations, they have the potential to significantly improve model accuracy, privacy, and real-time performance in decentralized settings. Future work needs to address these challenges for the broader deployment. As the research works are tested using software, the simulation results are utilized for comparative analysis, which is explained below.

III. Comparison of Performance in Various Techniques for Blockchain Integrated FI

The comparative analysis of various blockchain integrated FL, such as, Fog-IoT using FL with privacy preservation fraud data provider health care dataset [18], FedBlock Health [21], BFL-hIoT using Python 3 and the PyTorch library [25], PBDL conducted on Tyrone PC [27], Naive Bayes (NB), Decision Tree (DT), RF, SLSTM, and SLSTM (with Transformed) using Python and R programming language [45], FedTCN, Fed Simple RNN, FVC [48], and FedAvg [55] for data privacy based on their performance analysis in terms of accuracy, loss, detection rate, and root mean square error (RMSE) has been discussed in this section.

Figure 2 compares the accuracy of methods, such as Fog-IoT using FL, FedBlock Health, BFL-hIoT, and PBDL. The FedBlock Health method is shown to be the most accurate, with a 97.5% accuracy, surpassing all other techniques. BFL-hIoT closely follows with an accuracy of 95.0%, thus showing great performance too. Contrary to this, Fog-IoT achieves 85.0% in accuracy by using FL, and the lowest accuracy is that of PBDL, which is 82.5%. This indicates that

Table 5: Survey of FL based on blockchain for additional emerging uses

Ref No	Techniques used	Significance	Drawbacks
Zhao et al. [58]	FL, blockchain, and a reputation mechanism	Enables privacy-preserving ML training, helps manufacturers predict customer needs and behaviors	Potential bias in global models due to uniform contributions from diverse customers
ur Rehman et al. [59]	Fine-grained FL, blockchain	Decentralizes shared ML models, ensures trustworthy training, and addresses heterogeneity and efficiency	High computational overhead during model synchronization in heterogeneous edge environments
Li et al. [60]	Blockchain, FL, and committee consensus	Reduces consensus computing, improves scalability, security, and model storage	Delay in model updates in time-sensitive tasks due to network traffic
Zhang et al. [61]	Blockchain, FL, and smart agent architecture	Fully decentralized, privacy-preserving model for FL tasks, with smart agents acting as blockchain peers	Increased complexity in architecture, difficulty in managing, and synchronizing a decentralized network
Wang et al. [62]	Blockchain, FL, differential privacy, and self-reliability filter	Privacy-preserving with reduced communication overhead while maintaining model quality	Trade-off between privacy preservation and training accuracy due to differential privacy techniques
Qi et al. [63]	Consortium blockchain, FL, and differential privacy	Prevents unreliable updates and enhances privacy protection in FL for traffic flow prediction	Delays in real-time prediction performance due to reliance on miners for verification
Wang et al. [64]	Blockchain, FL, Multi-Krum, and homomorphic encryption	Provides secure and privacy-preserving model aggregation, incentivizes participation with reputation-based mechanisms	Significant computational overhead from homomorphic encryption, especially in low-resource environments
Moulaoui et al. [65]	Blockchain, FL, classification approaches, and model aggregation	Applied to VANET and ITS cyber-threat detection, improves classification model aggregation	Slow model aggregation, counter to the fast response needed in high-speed vehicle networks
Hua et al. [66]	Blockchain, FL, SVM, and historical driving data	Asynchronous collaborative ML between distributed agents, improves model accuracy	Limited scalability due to SVM's dependency, inadequate for complex real rail systems
Durga et al. [67]	Blockchain, FL, ensemble deep learning, and hybrid capsule learning network	Privacy-preserving data sharing improves prediction accuracy in health care applications	High computational complexity, performance issues in resource-constrained health care environments

FL, federated learning.

these methods are less effective. Thus, overall, the graph demonstrates that FedBlock Health and BFL-hIoT are significantly more accurate than the other approaches.

Figure 3 compares the loss values for different types of methods, including Fog-IoT using FL, FedBlock Health, BFL-hIoT, and PBDL. Here, it is evident that Fog-IoT using FL has the highest loss with 0.09 and poor performance. On the contrary, FedBlock Health, BFL-hIoT, and PBDL have had substantially smaller loss values, and each value is

around 0.02, which shows superior performance compared to the minimum loss they produce. The significant drop from Fog-IoT with FL to the other methods shows a large improvement in loss reduction achieved by FedBlock Health, BFL-hIoT, and PBDL.

Figure 4 represents the detection rates (%) of different methods, NB, DT, RF, SLSTM, and SLSTM (with Transformed). The highest detection rate is obtained by SLSTM (with Transformed) at 90%, thus proving its efficiency. SLSTM stands at 85%, which

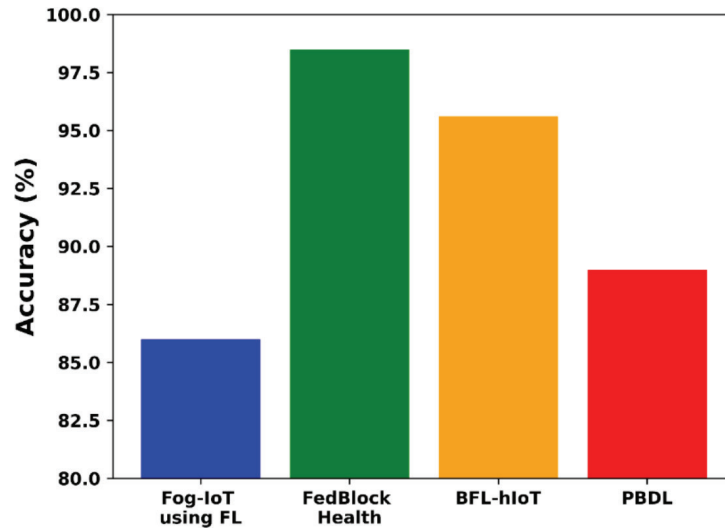


Figure 2: Comparison of accuracy. FL, federated learning.

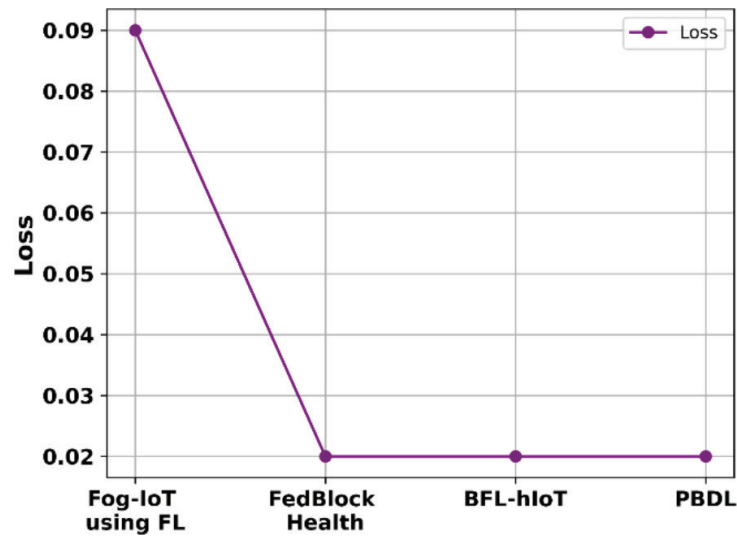


Figure 3: Comparison of loss. FL, federated learning.

proves its high accuracy. RF obtained a detection rate of 81%, which is more than that of DT, whose detection rate is 78%. NB records the lowest detection rate at 75%, making it stand out as the least potent method. The graph presents the effectiveness of SLSTM-based methods, especially their combination with transformations.

Figure 5 compares the RMSE of methods, such as FedAvg, FedTCN, Fed Simple RNN, and FVC. FedAvg has higher RMSE at around 0.65 and lower accuracy among the methods. FedTCN, Fed Simple RNN, and FVC achieve roughly RMSE values at

approximately 0.3, thereby bringing out an immense improvement over FedAvg's performance. The similar RMSE values of FedTCN, Fed Simple RNN, and FVC indicate that all these methods have similar levels of accuracy, with a slight advantage for FVC. This analysis shows that these specialized FL techniques, such as FVC, FedTCN, and Fed Simple RNN, are better than FedAvg in terms of the minimization of RMSE.

The F1-score of certain methods, namely, FedProX, FedNOVA, FedGP and FedAVG [68] are analyzed in Figure 6. Among them, FedNOVA attains the least F1-score of 0.718, while the FedGP has the

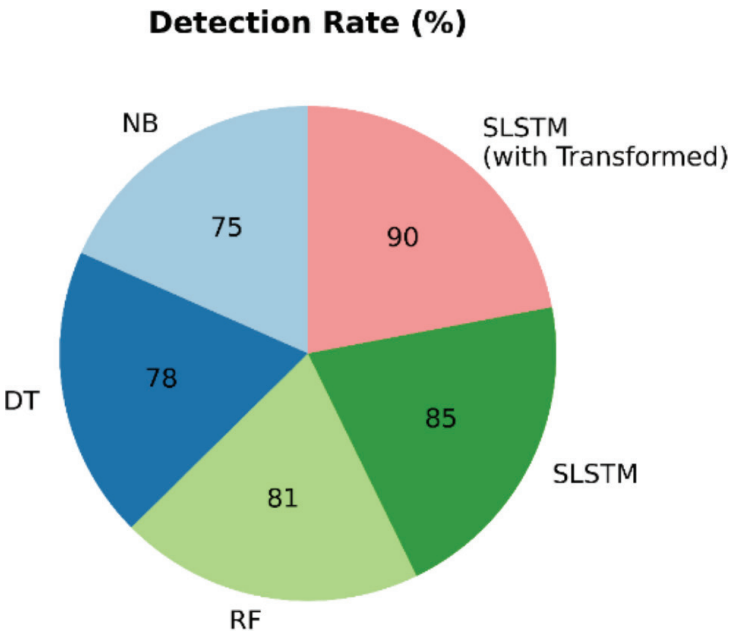


Figure 4: Comparison of detection rate. SLSTM, stacked long short-term memory.

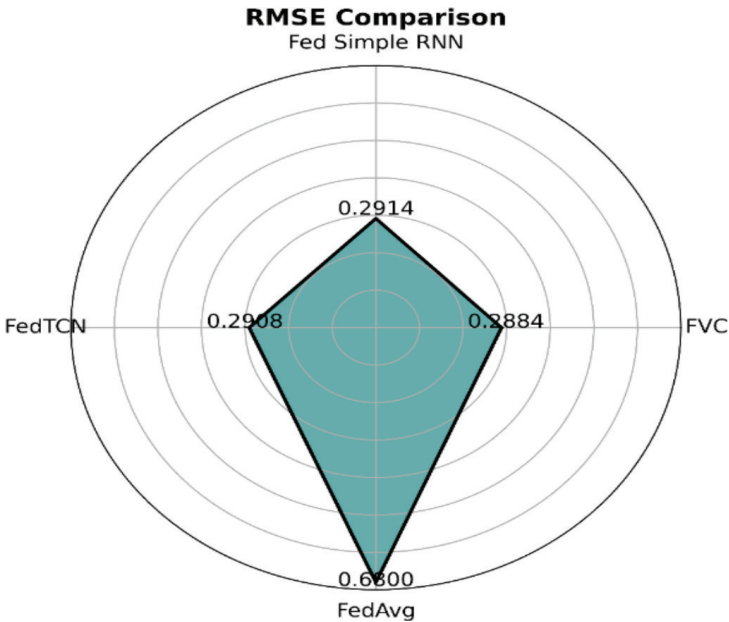


Figure 5: Comparison of RMSE. FVC, federated voting classifier; RMSE, root mean square error.

highest F1-score of 0.743. Meanwhile, the F1-scores of FedProX and FedAVG are 0.726 and 0.738, which are attained, respectively. This shows that the F1-scores of all the baseline models are between 0.71 and 0.75, with FedGP attaining the highest score. This indicates that the baseline models perform

similarly, with only small variations, which shows the increase in performance over FL methods.

Figure 7 provides the comparative analysis of various baseline models, such as FedProX, FedAvg, and FedNOVA [69], in terms of MSE. In this context, FedNOVA has the least MSE of 0.21, whereas

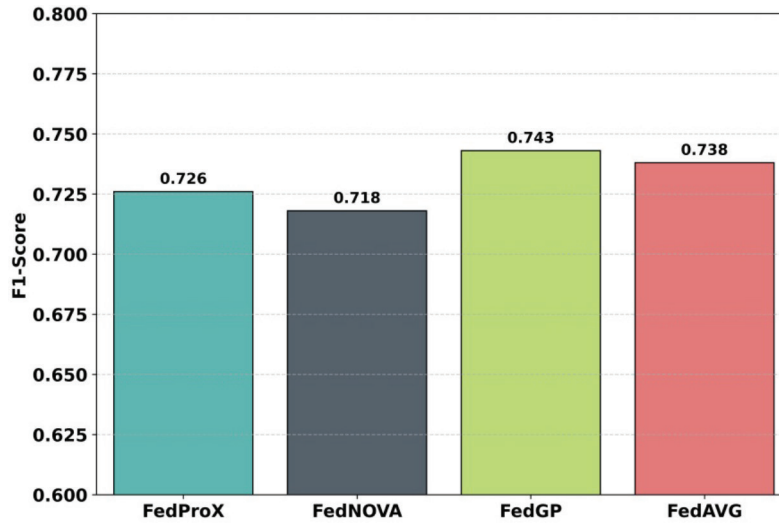


Figure 6: Comparison of F1-scores.

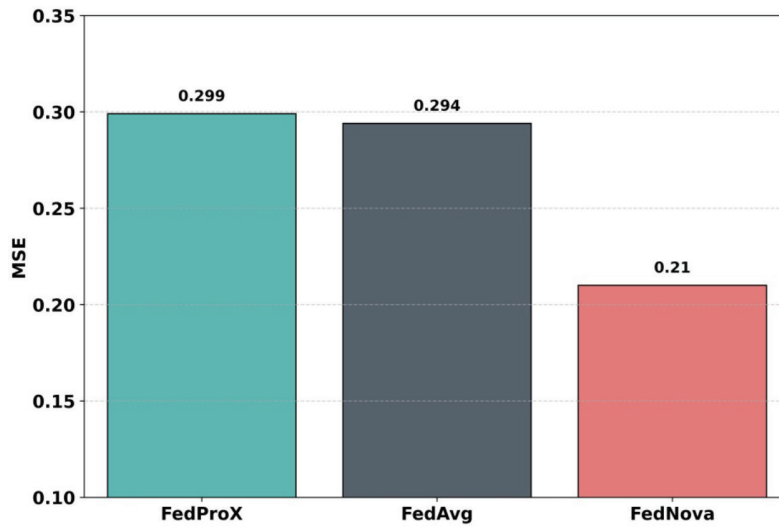


Figure 7: Comparison of Mean Squared Error (MSE).

the FedProX has the highest MSE of 0.299, which is followed by FedAvg with MSE of 0.294. FedNOVA achieves the best performance with the least MSE, compared with other models, with a more stable and accurate convergence behavior by minimizing prediction errors under the given data distribution and federated setting. Meanwhile, FedProX and FedAvg exhibit higher prediction deviations, reflecting comparatively weaker optimization performance. This comparative analysis of the performance metrics revealed that the models are tested using simulation rather than in real time.

IV. Result and Summary

The application of blockchain-enabled FL across various domains like health care, smart cities, smart agriculture, and smart grids has shown considerable potential but also presents several challenges. The analyzed summary of various blockchain-enabled FL applications is as follows:

- The integration of blockchain with FL ensures the privacy and security of medical data during collaborative model training. The combination enhances

data integrity, reduces the risk of data breaches, and supports compliance with privacy regulations. However, challenges, such as high computational overhead, latency in model synchronization, and issues with scalability in decentralized systems, remain significant.

- Blockchain-enhanced FL offers secure and efficient data sharing between various smart city components, such as sensors, traffic systems, and utility grids. This integration ensures data consistency and trustworthiness, enabling better resource management. However, issues, such as system scalability, communication overhead, and delays due to the consensus process in blockchain, remain critical obstacles to widespread adoption.
- In smart agriculture, FL combined with blockchain can optimize farming practices by securely sharing data across distributed systems for crop monitoring and resource management. This helps in enhancing predictive models for agricultural yields and resource use. The primary challenges in this domain include the energy consumption of blockchain systems, and the complexity of model updates in decentralized settings.
- Blockchain and FL together offer the potential for secure, real-time data exchange and privacy-preserving energy management in smart grids. This combination ensures data transparency and supports optimization in grid operations. However, latency issues in time-sensitive data updates and scalability concerns regarding large-scale implementation in real-world smart grid systems need to be addressed.
- Blockchain and FL are being explored in other emerging fields, such as autonomous vehicles, IoT networks, and industrial automation. These technologies ensure privacy and integrity in the decentralized learning process while offering real-time data sharing. However, these applications still face challenges, such as maintaining real-time processing capabilities, model synchronization, and managing system complexity across diverse environments.
- The integration of blockchain with FL solutions into legacy health care and energy systems introduces migration barriers, such as latency, compliance, and hardware constraints, which limit real-world deployment. However, the integration is feasible with middleware bridges, lightweight consensus protocols, edge-optimized FL models, and hybrid logging architectures.

- In addition to accuracy, privacy, and latency in blockchain operations, some works addressed significant computational and energy overheads, especially in resource-constrained environments. This overhead directly affects feasibility, device lifetime, and deployment scalability, which should be considered as a significant metric in future works.

V. Conclusion

In this research, a complete survey was done to observe the integration of blockchain-enabled FL across a variety of domains, ranging from health care, smart cities, smart agriculture, smart grids, and many other emerging applications. The survey went through existing methods, benefits, and challenges, noting how blockchain enhances FL in terms of data security, privacy preservation, and trust in decentralized systems. More precisely, the surveyed domains indicated improved collaborative learning and data protection, but they suffered from challenges of scalability, computational overhead, and latency. Moreover, analyzing these techniques shows the potential, as well as the limitations, when applied to real-world cases, with a focus on the need for optimized synchronization and adaptive solutions. The conclusions outline the importance of blockchain-enabled FL in addressing domain-specific problems despite pointing out areas that need to be further refined to solve current issues. This survey outlined some critical insights into the convergence of blockchain and FL, presenting a comprehensive understanding of their methodologies, importance, and limitations. It will help researchers and practitioners gain further knowledge about the potential and challenges in this evolving field, fostering future innovations and advancements, which can address identified gaps more effectively.

VI. Future Scope

From the above-mentioned limitations, the research can be developed in the future by analyzing each direction. Future research can be done based on the following suggestions:

- In health care and IoT applications, lightweight FL frameworks can be developed by including sparsified models and knowledge distillation to reduce computational overheads for resource-constrained devices. For heterogeneous devices

and imbalanced workloads, adaptive load-balancing algorithms can be implemented to ensure equal distribution of tasks, while energy-efficient training schedules can minimize power consumption. Asynchronous FL techniques combined with blockchain sharding can address issues in real-time model synchronization and performance.

- By integrating advanced technologies, AI, scalability issues in blockchain models (which are not inherently due to blockchain alone) can be mitigated. Additionally, architecture redesigning could improve the scalability, which is proven in sharding, Directed Acyclic Graph (DAG)-based ledgers, and lightweight Byzantine Fault Tolerance (BFT) consensus.
- For smart cities, hierarchical FL models integrated with multi-layer blockchain networks can be implemented to effectively manage scalability. Real-time operation latency could be eliminated through reinforcement learning techniques such as task prioritization and dynamic resource allocation. Energy efficiency will also be guaranteed by the low-power edge computing frameworks, which utilize ultra-low-energy processors to execute workloads.
- In smart agriculture, federated transfer learning with mechanisms of consensus-based blockchain mechanisms can enhance scalability and multi-party conflict resolution. Incorporation of quantized models and collaboration between the edge and cloud can reduce latency and high computational demands. Dynamic data handling can be improved by the use of incremental learning techniques that update the models using real-time data while keeping data integrity with the use of blockchain logging.
- In smart grids, federated reinforcement learning combined with blockchain-based consortium architectures can distribute the computational tasks, thus eliminating scalability and computational load problems. Blockchain gateways can help in interoperability with legacy systems for efficient data exchange. Model optimization techniques, such as pruning, sparsification, and lightweight encryption protocols can be used to operate resource-constrained edge devices smoothly without excessive computational demand.
- Use parameter server architectures combined with blockchain sidechains to effectively update models, which reduce the high computational overhead during model synchronization. Hybrid encryption techniques such as functional encryption and par-

tially homomorphic encryption can be used to find a balance between privacy and accuracy of the model. Slow aggregation due to network delays may be overcome by using 5G-enabled communication protocols and by implementing distributed aggregation mechanisms for enhanced real-time performance and reliability.

- Furthermore, to evaluate lightweight FL and blockchain sharding, the recommended simulation and controlled field deployments are listed below. Simulations can be performed using tools such as, NS-3, Hyperledger Caliper, or FL simulators like Flower/FedML that enhance stress-testing scalability, communication load, shared configuration, and consensus latency under large network sizes. They assist in rapid experimentation with heterogeneous clients and adversarial scenarios.

References

- [1] Ahammed, M.F. and Labu, M.R., 2024. Privacy-preserving data sharing in healthcare: advances in secure multiparty computation. *Journal of Medical and Health Studies*, 5(2), pp. 37-47.
- [2] Du, R., 2025. A study on local differential privacy under adverse circumstances.
- [3] Odeh, A., Abdelfattah, E. and Salameh, W., 2024. Privacy-preserving data sharing in telehealth services. *Applied Sciences*, 14(23), p.10808.
- [4] Chandra, A., 2024. Privacy-preserving data sharing in cloud computing environments. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, 13(1), pp. 104-111.
- [5] Dhinakaran, D., Sankar, S.M., Selvaraj, D. and Raja, S.E., 2024. Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration. *arXiv preprint arXiv:2401.00794*.
- [6] Li, K., Lohachab, A., Dumontier, M. and Urovi, V., 2025. Privacy preservation in blockchain-based health-care data sharing: A systematic review. *Peer-to-Peer Networking and Applications*, 18(6), pp. 1-53.
- [7] Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A. and Verykios, V.S., 2024. Privacy-preserving techniques in generative ai and large language models: a narrative review. *Information*, 15(11), p.697.
- [8] Rahman, A., Iqbal, A., Ahmed, E. and Ontor, M.R.H., 2024. Privacy-preserving machine learning: techniques, challenges, and future directions in safeguarding personal data management. *International journal of business and management sciences*, 4(12), pp. 18-32.

- [9] Shahsavari, Y., Dambri, O.A., Baseri, Y., Hafid, A.S. and Makrakis, D., 2024. Integration of Federated Learning and Blockchain in Healthcare: A Tutorial. *arXiv preprint arXiv:2404.10092*.
- [10] Malik, R., Razzaq, H., Bhatt, C., Kaushik, K. and Khan, I.U., 2024, May. Advancing Healthcare IoT: Blockchain and Federated Learning Integration for Enhanced Security and Insights. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 308-314). IEEE.
- [11] Pandya, S., Srivastava, G., Jhaveri, R., Babu, M.R., Bhattacharya, S., Maddikunta, P.K.R., Mastorakis, S., Piran, M.J. and Gadekallu, T.R., 2023. Federated learning for smart cities: A comprehensive survey. *Sustainable Energy Technologies and Assessments*, 55, p.102987.
- [12] Ahmed, R.A., Hemdan, E.E.D., El-Shafai, W., Ahmed, Z.A., El-Rabaie, E.S.M. and Abd El-Samie, F.E., 2022. Climate-smart agriculture using intelligent techniques, blockchain and Internet of Things: Concepts, challenges, and opportunities. *Transactions on Emerging Telecommunications Technologies*, 33(11), p.e4607.
- [13] Zhang, Z., Rath, S., Xu, J. and Xiao, T., 2024. Federated Learning for Smart Grid: A Survey on Applications and Potential Vulnerabilities. *arXiv preprint arXiv:2409.10764*.
- [14] Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Hammoudeh, M., Karimipour, H. and Srivastava, G., 2022. Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. *IEEE Transactions on Industrial Informatics*, 18(11), pp. 8356-8366.
- [15] Kalapaaking, A.P., Khalil, I., Rahman, M.S., Atiquzzaman, M., Yi, X. and Almashor, M., 2022. Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. *IEEE Transactions on Industrial Informatics*, 19(2), pp. 1703-1714.
- [16] Ghaly, M., Elbeltagi, E., Elsmadony, A. and Tantawy, M.A., 2024. Integration of Blockchain-Enabled smart contracts in construction: SWOT framework and social network analysis. *Civil Engineering Journal*, 10(05), pp. 1662-1697.
- [17] Ehab, A., Mahdi, M.A. and El-Helloty, A., 2024. BIM maintenance system with IoT integration: enhancing Building performance and facility management. *Civ. Eng. J*, 10, pp. 1953-1973.
- [18] Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A. and Wang, W., 2022. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics*, 27(2), pp. 664-672.
- [19] Baucas, M.J., Spachos, P. and Plataniotis, K.N., 2023. Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. *IEEE Transactions on Computational Social Systems*, 10(4), pp. 1732-1741.
- [20] Rahman, M.A., Hossain, M.S., Islam, M.S., Alrajeh, N.A. and Muhammad, G., 2020. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *IEEE Access*, 8, pp. 205071-205087.
- [21] Alshudukhi, K.S., Ashfaq, F., Jhanjhi, N. and Humayun, M., 2024. Blockchain-Enabled Federated Learning for Longitudinal Emergency Care. *IEEE Access*.
- [22] Alsamhi, S.H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., Wei, X., Guizan, M. and Curry, E., 2024. Federated learning meets blockchain in decentralized data-sharing: Healthcare use case. *IEEE Internet of Things Journal*.
- [23] Waheed, N., Rehman, A.U., Nehra, A., Farooq, M., Tariq, N., Jan, M.A., Khan, F., Alalmaie, A.Z. and Nanda, P., 2023, December. Fedblockhealth: A synergistic approach to privacy and security in IoT-enabled healthcare through federated learning and blockchain. In *GLOBECOM 2023-2023 IEEE Global Communications Conference* (pp. 3855-3860). IEEE.
- [24] Ahmed, S.T., Mahesh, T.R., Srividhya, E., Vinoth Kumar, V., Khan, S.B., Albuali, A. and Almusharraf, A., 2024. Towards blockchain based federated learning in categorizing healthcare monitoring devices on artificial intelligence of medical things investigative framework. *BMC Medical Imaging*, 24(1), p.105.
- [25] Ganapathy, G., Anand, S.J., Jayaprakash, M., Lakshmi, S., Priya, V.B. and Pandi, S., 2024. A blockchain based federated deep learning model for secured data transmission in healthcare lot networks. *Measurement: Sensors*, 33, p.101176.
- [26] Ali, A., Al-Rimy, B.A.S., Tin, T.T., Altamimi, S.N., Qasem, S.N. and Saeed, F., 2023. Empowering precision medicine: Unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. *Sensors*, 23(17), p.7476.
- [27] Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Islam, A.N. and Shorfuzzaman, M., 2022. Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics*, 18(11), pp. 8065-8073.
- [28] Hai, T., Wang, D., Seetharaman, T., Amelesh, M., Sreejith, P.M., Sharma, V., Ibeke, E. and Liu, H., 2023,

February. A novel & innovative blockchain-empowered federated learning approach for secure data sharing in smart city applications. In *International Conference on Advances in Communication Technology and Computer Engineering* (pp. 105-118). Cham: Springer Nature Switzerland.

[29] Abbas, S.M.A., Khan, M.A., Boulila, W., Kouba, A., Khan, M.S. and Ahmad, J., 2024. UAVs and Blockchain Synergy: Enabling Secure Reputation-based Federated Learning in Smart Cities. *IEEE Access*.

[30] Guo, S., Xiang, B., Xia, X., Yan, Z. and Li, Y., 2020. Blockchain and federated learning based data security sharing mechanism over smart city.

[31] Qolomany, B., Ahmad, K., Al-Fuqaha, A. and Qadir, J., 2020, December. Particle swarm optimized federated learning for industrial IoT and smart city services. In *GLOBECOM 2020-2020 IEEE Global Communications Conference* (pp. 1-6). IEEE.

[32] Kumar, P., Gupta, G.P. and Tripathi, R., 2021. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *Journal of Systems Architecture*, 115, p.101954.

[33] Abdel-Basset, M., Alrashdi, I., Hawash, H., Sallam, K. and Hameed, I.A., 2023. Towards efficient and trustworthy pandemic diagnosis in smart cities: a blockchain-based federated learning approach. *Mathematics*, 11(14), p.3093.

[34] Muhammad, M.H.G., Ahmad, R., Fatima, A., Mohammed, A.S., Raza, M.A. and Khan, M.A., 2024. Secure and transparent traffic congestion control system for smart city using a federated learning approach.

[35] Yin, X., Qiu, H., Wu, X. and Zhang, X., 2024. An Efficient Attribute-Based Participant Selecting Scheme with Blockchain for Federated Learning in Smart Cities. *Computers*, 13(5), p.118.

[36] Padma, A. and Ramaiah, M., 2024. Blockchain based an efficient and secure privacy preserved framework for smart cities. *IEEE Access*.

[37] Far, A.Z., Far, M.Z., Gharibzadeh, S., Zangeneh, S., Amini, L. and Rahimi, M., 2024. Artificial Intelligence for Secured Information Systems in Smart Cities: Collaborative IoT Computing with Deep Reinforcement Learning and Blockchain. *arXiv preprint arXiv:2409.16444*.

[38] Shen, R., Zhang, H., Chai, B., Wang, W., Wang, G., Yan, B. and Yu, J., 2024. BAFL-SVM: A blockchain-assisted federated learning-driven SVM framework for smart agriculture. *High-Confidence Computing*, p.100243.

[39] Praharaj, L., Gupta, M. and Gupta, D., 2023, December. Hierarchical Federated Transfer learning

and Digital Twin Enhanced Secure Cooperative Smart Farming. In *2023 IEEE International Conference on Big Data (BigData)* (pp. 3304-3313). IEEE.

[40] Singh, S.K., Kumar, M., Khanna, A. and Virdee, B., 2024. Blockchain and FL-based secure architecture for enhanced external Intrusion detection in smart farming. *IEEE Internet of Things Journal*.

[41] Vimalajeewa, D., Kulatunga, C., Berry, D.P. and Balasubramaniam, S., 2021. A service-based joint model used for distributed learning: Application for smart agriculture. *IEEE Transactions on Emerging Topics in Computing*, 10(2), pp.838-854.

[42] Leduc, G., Kubler, S. and Georges, J.P., 2021. Innovative blockchain-based farming marketplace and smart contract performance evaluation. *Journal of Cleaner Production*, 306, p.127055.

[43] Hasan, H.R., Musamih, A., Salah, K., Jayaraman, R., Omar, M., Arshad, J. and Boscovic, D., 2024. Smart agriculture assurance: IoT and blockchain for trusted sustainable produce. *Computers and Electronics in Agriculture*, 224, p.109184.

[44] Chaganti, R., Varadarajan, V., Gorantla, V.S., Gadekallu, T.R. and Ravi, V., 2022. Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture. *Future Internet*, 14(9), p.250.

[45] Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Gadekallu, T.R. and Srivastava, G., 2021. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. *Computer Networks*, 187, p.107819.

[46] Pranto, T.H., Noman, A.A., Mahmud, A. and Haque, A.B., 2021. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Computer Science*, 7, p.e407.

[47] Sakthi, U. and DafniRose, J., 2022. Blockchain-enabled smart agricultural knowledge discovery system using edge computing. *Procedia Computer Science*, 202, pp.73-82.

[48] Ashraf, M.M., Waqas, M., Abbas, G., Baker, T., Abbas, Z.H. and Alasmay, H., 2022. Feddp: A privacy-protecting theft detection scheme in smart grids using federated learning. *Energies*, 15(17), p.6241.

[49] Zhang, S., Rong, J. and Wang, B., 2020. A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. *International Journal of Electrical Power & Energy Systems*, 121, p.106140.

[50] Yilmaz, I., Kapoor, K., Siraj, A. and Abouyoussef, M., 2021, April. Privacy protection of grid users data with blockchain and adversarial machine learning. In *proceedings of the 2021 ACM workshop on secure and trustworthy cyber-physical systems* (pp. 33-38).

- [51] Fan, H., Liu, Y. and Zeng, Z., 2020. Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain. *Sensors*, 20(18), p.5282.
- [52] Lu, W., Ren, Z., Xu, J. and Chen, S., 2021. Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid. *IEEE Transactions on Network and Service Management*, 18(2), pp. 1246-1259.
- [53] Jithish, J., Alangot, B., Mahalingam, N. and Yeo, K.S., 2023. Distributed anomaly detection in smart grids: a federated learning-based approach. *IEEE Access*, 11, pp. 7157-7179.
- [54] Su, Z., Wang, Y., Luan, T.H., Zhang, N., Li, F., Chen, T. and Cao, H., 2021. Secure and efficient federated learning for smart grid with edge-cloud collaboration. *IEEE Transactions on Industrial Informatics*, 18(2), pp. 1333-1344.
- [55] Fekri, M.N., Grolinger, K. and Mir, S., 2022. Distributed load forecasting using smart meter data: Federated learning with Recurrent Neural Networks. *International Journal of Electrical Power & Energy Systems*, 137, p.107669.
- [56] Li, Y., Wei, X., Li, Y., Dong, Z. and Shahidehpour, M., 2022. Detection of false data injection attacks in smart grid: A secure federated deep learning approach. *IEEE Transactions on Smart Grid*, 13(6), pp. 4862-4872.
- [57] Shrestha, R., Mohammadi, M., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., Sanz, A.L., Nowroozi, E. and Lindgren, A., 2024. Anomaly detection based on lstm and autoencoders using federated learning in smart electric grid. *Journal of Parallel and Distributed Computing*, 193, p.104951.
- [58] Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., Lyu, L. and Liu, Y., 2020. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal*, 8(3), pp. 1817-1829.
- [59] ur Rehman, M.H., Salah, K., Damiani, E. and Svetinovic, D., 2020, July. Towards blockchain-based reputation-aware federated learning. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 183-188). IEEE.
- [60] Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z. and Yan, Q., 2020. A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, 35(1), pp. 234-241.
- [61] Zhang, Z., Yang, T. and Liu, Y., 2020. SABlockFL: a blockchain-based smart agent system architecture and its application in federated learning. *International Journal of Crowd Science*, 4(2), pp. 133-147.
- [62] Wang, R., Li, H. and Liu, E., 2021. Blockchain-based federated learning in mobile edge networks with application in internet of vehicles. *arXiv preprint arXiv:2103.01116*.
- [63] Qi, Y., Hossain, M.S., Nie, J. and Li, X., 2021. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, 117, pp. 328-337.
- [64] Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X. and Guizani, M., 2024. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digital Communications and Networks*, 10(1), pp. 126-134.
- [65] Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S. and Rizwan, M., 2023. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems*, 40(5), p. e13103.
- [66] Hua, G., Zhu, L., Wu, J., Shen, C., Zhou, L. and Lin, Q., 2020. Blockchain-based federated learning for intelligent control in heavy haul railway. *IEEE Access*, 8, pp. 176830-176839.
- [67] Durga, R. and Poovammal, E., 2022. Fled-block: Federated learning ensembled deep learning blockchain model for covid-19 prediction. *Frontiers in Public Health*, 10, p.892499.
- [68] de Vega, F.F. and Calvaresi, D., Genetic Programming in Federated Aggregation: A comparison of FedGP with State of the Art Methods.
- [69] Deng, J., Cai, S., Wu, W., Jiang, R., Deng, H., Ma, J. and Luo, Y., 2025. A Cross-Regional Load Forecasting Method Based on a Pseudo-Distributed Federated Learning Strategy. *IEEE Access*.