future internet

MDPI

Review

Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions

Muneerah Al Asqah * and Tarek Moulahi *

Department of Information Technology, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia
* Correspondence: 411207283@qu.edu.sa (M.A.A.); t.moulahi@qu.edu.sa (T.M.)

Abstract: The Internet of Things (IoT) compromises multiple devices connected via a network to perform numerous activities. The large amounts of raw user data handled by IoT operations have driven researchers and developers to provide guards against any malicious threats. Blockchain is a technology that can give connected nodes means of security, transparency, and distribution. IoT devices could guarantee data centralization and availability with shared ledger technology. Federated learning (FL) is a new type of decentralized machine learning (DML) where clients collaborate to train a model and share it privately with an aggregator node. The integration of Blockchain and FL enabled researchers to apply numerous techniques to hide the shared training parameters and protect their privacy. This study explores the application of this integration in different IoT environments, collectively referred to as the Internet of X (IoX). In this paper, we present a state-of-the-art review of federated learning and Blockchain and how they have been used in collaboration in the IoT ecosystem. We also review the existing security and privacy challenges that face the integration of federated learning and Blockchain in the distributed IoT environment. Furthermore, we discuss existing solutions for security and privacy by categorizing them based on the nature of the privacy-preservation mechanism. We believe that our paper will serve as a key reference for researchers interested in improving solutions based on mixing Blockchain and federated learning in the IoT environment while preserving privacy.

Keywords: Blockchain; federated learning; Internet of Things; privacy

Citation: Al Asqah, M.; Moulahi, T. Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions. *Future Internet* **2023**, *15*, 203. https://doi.org/10.3390/fi15060203

Academic Editor: Claude Chaudet

Received: 3 May 2023
Revised: 26 May 2023
Accepted: 30 May 2023
Published: 31 May 2023

1. Introduction

Modern life includes technology incorporated with everyday tasks in all shapes and forms. Starting from industrial fields and ending up in smart homes, the Internet of Things (IoT) has become an irreplaceable technology that greatly improves our daily life. One example of an IoT application is Industrial IoT (IIoT), where the technologies of IoT are applied to manage and automate the job of controlling industrial equipment [1]. Another example is the application of health sensors and readers, which can be called the Internet of Health Things (IoHT). All the different IoT environments follow the same concepts of analyzing raw data flow and can be referred to as the Internet of X things (IoXT).

The number of connected devices that receive and send data in the IoT is unlimited. According to statistics, the number of connected IoT devices may reach 19.1 billion in 2025 [2]. This high number demonstrates the strong growth of IoT technologies, devices, and systems in many application areas. IoT is a technology that comprises other technologies and devices that collect, transfer, and process data. Researchers have used several IoT reference models. Table 1 shows the seven-layer model with each layer's components [3].

As its first layer of communications, the IoT starts with sensors, radio frequency identification (RFID) readers, actuators, and other low-level devices that collect raw data and forward them to the higher layers in the interrelated network. The next hop of communication is the more intelligent edge nodes [4], which are devices with higher computational

capabilities responsible for the first phase of processing the IoT raw data. Later on, cloud-computing layers are applied to provide the low-level IoT resource-constrained hardware devices additional computation and storage capabilities [5]. Figure 1 presents a high-level overview of the cloud IoT ecosystem [4]. However, more in-depth analysis layers can be included to process the raw IoT data.

Table 1. CISCO's IoT reference model [3].

#	Layer Name	Component
7	Collaboration and Processes	People and Business Processes
6	Application	Reporting, Analytics, Control
5	Data Abstraction	Aggregation and Access
4	Data Accumulation	Storage
3	Edge (Fog) Computing	Data Element Analysis and Transformation
2	Connectivity	Communication and Processing Units
1	Physical Devices and Controllers	The "Things" in IoT

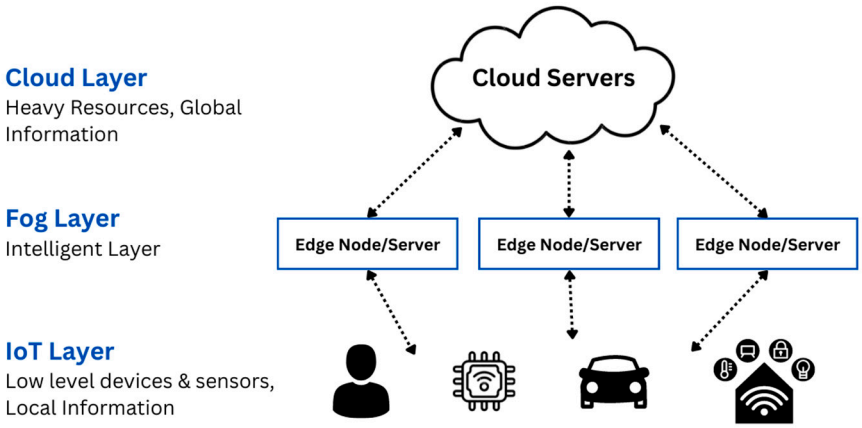

Figure 1. The interaction diagram of IoT, fog, and cloud layers.

Data flow from the IoT devices to the centralized cloud layer for analysis, and the analysis results travel back to the IoT devices. This flow puts a heavy transmission cost on the network, and to address this issue, edge computing, or the fog layer, was introduced; it started as a content delivery network (CDN) component. CDN security issues have been discussed in [5], and the "edge" addresses transmission and storage issues.

The distributed architecture of edge nodes and the need to analyze the large amounts of raw data have led to a research direction which aims to develop approaches that integrate machine learning (ML) into the IoT edge system [6]. Federated learning, which belongs to the family of decentralized machine learning (DML), is a collaborative learning model where nodes share and train a unified model with an aggregator node [7].

Federated learning addresses the need for computing the IoT data [8], but federated learning alone cannot guarantee the integrity and privacy of raw data traveling among clients and aggregated nodes. Blockchain is the technology of nodes that share a distributed ledger of transactional information, which is designed to ensure means of integrity and privacy [9]. The strong characteristics of Blockchain encouraged researchers to develop ways to integrate it with federated learning to preserve data integrity and privacy.

Research contributions of this work

We summarize the main contributions of this work as follows:

1. We present a state-of-the-art review of federated learning and Blockchain and how they have been used in collaboration in the IoT ecosystem.
2. We review the existing security and privacy challenges that face the integration of federated learning and Blockchain in the distributed IoT environment.

3. We discuss existing solutions for security and privacy by categorizing them based on the nature of the privacy-preservation mechanism.

We organize the rest of this paper as follows. The next section reviews recent surveys that covered the integration of federated learning and Blockchain for IoT security and privacy. Section 3 presents a state-of-the-art review of Blockchain and federated learning. In Section 4, we discuss the integration challenges these technologies would face in an IoT environment. In Section 5, we categorize proposed solutions aimed at solving security and privacy challenges. Finally, we discuss outstanding research challenges that must be addressed in the future in the area of Blockchain and federated learning integration for the IoT environment to preserve privacy and security.

2. Related Work

The trend of integrating federated learning and Blockchain is still fairly new. Consequently, there are not many works in the literature that summarize the combination of both technologies in IoT from a security perspective.

The authors of [10] presented a comprehensive survey that investigated the security and privacy concerns of Blockchain and FL (BCFL) integrations. They studied the functions of BCFL elements including verification mechanisms, model aggregation, and incentive mechanisms. In addition, the authors analyzed current BCFL security and privacy challenges.

The authors of [11] presented a systematic survey that reviewed the Blockchain-based federated learning approaches from a security and privacy perspective. The authors presented state-of-the-art results of combining federated learning and Blockchain while studying relevant security and privacy concerns. Although the work of [10,11] were thorough, they did not review works from an IoT perspective.

However, the authors of [12] presented a survey of Blockchain and federated learning integration in IoT. They provided a review of the Blockchain, federated learning, and IoT taxonomy while considering basic security and privacy concerns.

In [13], the authors proposed a comprehensive survey discussing the use of FL techniques to secure IoT-based systems. They also outlined existing solutions and future trends related to IoT data. In their paper, the authors discussed security and privacy issues in the IoT ecosystem. The research works in [14–16] discussed the use of federated learning and Blockchain in the Internet of Vehicles (IoV). The authors outlined existing solutions that deal with applying FL and Blockchain for security and privacy-preserved methods in the IoV ecosystem. In [14], the authors proposed a solution that used homomorphic encryption in addition to FL and Blockchain. Their aim was to improve the privacy preservation of user data. In [15], the authors presented a comprehensive survey that aimed to discuss existing solutions in the field of IoV. In addition, they presented the challenges and future trends for methods aimed at dealing with the privacy issues in the IoV.

Table 2 summarizes the discussed work with their limitations.

Table 2. Summary of related work.

Related Work	Summary	Limitation
[10]	Studied the security and privacy issues of Blockchain and federated learning integration.	Did not cover integrations related to IoT. Furthermore, no consideration on poisoning attack mitigations.
[11]	Explained federated learning approaches with concern to privacy and security issues.	The wide scope of the paper did not focus on IoT-related integrations, with no mention of poisoning attack mitigations.
[12]	Presented a survey that studied the integration between Blockchain, federated learning, and IoT with studying.	Did not provide analysis on the found literature and how the poisoning attacks are mitigated.
[13]	Propose a comprehensive survey discussing the use of FL techniques to secure IoT-based systems.	Did not outline adversarial machine learning attacks and how to tackle them.

Table 2. *Cont.*

Related Work	Summary	Limitation
[14]	The authors outlined existing solutions that deal with applying FL and Blockchain for security and privacy-preserved methods in the IoV ecosystem.	Focused only on IoV data and did not discuss other types of IoT ecosystems.
[15]		
[16]		
This paper	Provided a technology summary and reviewed existing integrations of Blockchain, federated learning, and IoT while performing a security and privacy analysis of each reference found in the literature.	-

In [9], the authors discussed the Blockchain trends in a general way and did not give high priority to privacy-preservation issues. The work of [10] lacked integrations related to IoT. In addition, the authors did not discuss the poisoning attacks that could happen in the learning phases. The main drawbacks of [11] are also discussing privacy and security issues based on federated learning, but this work did not consider the IoT specificities. Finally, in [12], the authors did not debate how the poisoning attacks are mitigated.

Although it is close to this paper's scope, the work of [12] did not review existing solutions that mitigate the poisoning attack threat. Furthermore, compared to [13–15], we believe that this paper is the first to study and review Blockchain integration with federated learning in IoT with a perspective on data and model poisoning attacks.

3. Federated Learning and Blockchain: Brief Review

In this paper, we study the integration of multiple powerful technologies that enhance efficiency, security, and privacy. The rest of this section reviews the main concepts of federated learning and Blockchain and how they are integrated into an IoT-based environment.

3.1. Federated Learning

Federated learning is a new technology that orchestrates connected clients to gain knowledge collaboratively. It was first introduced by Google in 2015 [17] to overcome three main issues: the huge amount of data gathered from many devices is unbalanced, non-independent and identically distributed (non-IID); the communication overhead of distant and massively distributed devices; and the insecure centralized data-storing mechanisms [10].

In federated learning, the learning burden is shared among connected nodes, usually referred to as clients, to train the ML model locally and upload the learning gradients to a central aggregator that levels all the learning gradients to a shared global model.

Figure 2 shows the basic topology of the federated learning procedure. It includes the list of clients selected to join the process by training the models locally. The aggregator is a central trusted server that could provide the aggregation results. Many communications can happen between different clients and the aggregator server. The process of FL is started by selecting clients, and next choosing the model. After performing the local training, the results will be sent to the aggregator server where they are aggregated. A global update can be performed next from the server and sent to the different clients. Figure 2 can be described by these five essential steps:

1. Clients selection: Participants' devices are selected to join the training iterations. This selection could depend on a number of factors, such as device processing capabilities and storage capacity, and is determined by definitive selection protocols [10].
2. Model selection: The primary model is chosen, and its main parameters are determined and shared with clients to start the federated learning [12].
3. Local model training: Clients independently train the model with the local device data storage [7].
4. Local model gradients updates: After each iteration, clients push the training gradients to the aggregator device [10].

5. Global model update: The aggregator applies an aggregation technique to level the trained model gradients and propagate the update to the clients to start the next round [7].

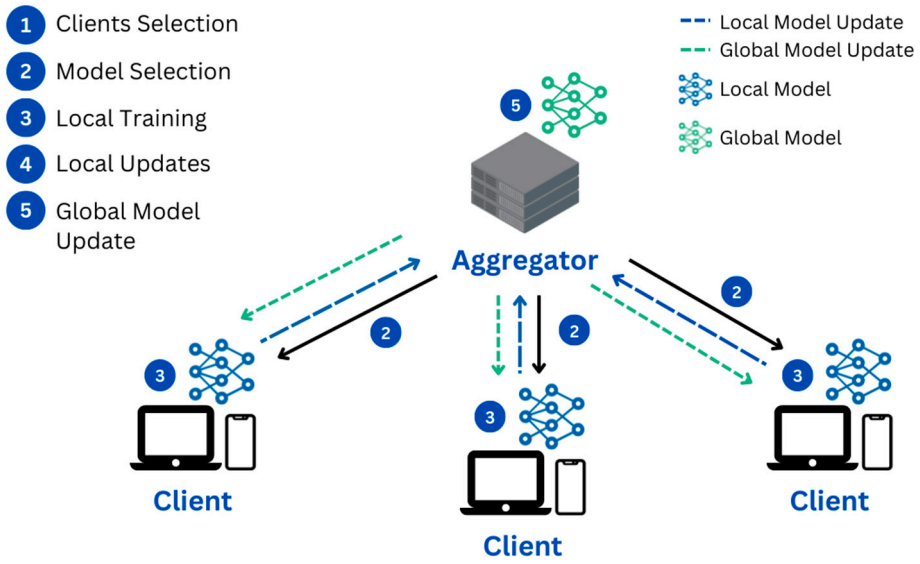

Figure 2. Basic topology of traditional federated learning.

3.1.1. Categories of Federated Learning

In the literature, federated learning is categorized in two ways; one categorization is based on how the data are distributed [18], and the other is based on the network architecture [12]. The three data distribution categories are as follows:

- Horizontal federated learning: Where the datasets have the exact same features but varying samples.
- Vertical federated learning: Where the sample space is the same, but the features are different.
- Federated transfer learning: Starts from a pre-trained model where the overlap of the samples space and features space is less.

Based on how the devices are connected in the FL environment, it can be further classified as one of the following approaches:

- Centralized approach: Where a global central model is updated by aggregating the clients' training parameters. This approach applies protocols to avoid malicious clien participation
- Decentralized approach: Where the clients' complete reliance on their neighbours to update the model removes the central authority. This approach requires absolute trust among clients.

3.1.2. Aggregation Techniques

Multiple algorithms are used to level the results from multiple participants' clients. Table 3 summarizes three of the most used aggregation techniques. We discuss the most relevant aggregation techniques, which are (1) FedAvg, which is based on calculating the parameters' average based on stochastic gradient descent (SGD); (2) SMC-Avg, which is characterized by its good performance even with 33% non-participated clients; and finally, (3) FedProx, which is derived from FedAvg, which can be applied in the case of heterogonous devices.

Table 3. Aggregation algorithms [13].

Algorithm	Based on	Centralized	Remarks
Federated Average (FedAvg)	Stochastic gradient descent (SGD)	√	-
Secure Multi-Party Computation (SMC-Avg)	-	√	Performs well even with 33% non-participating clients.
FedProx	FedAvg	√	Addresses device heterogeneity.

3.2. Blockchain Technology

Blockchain began after the publication of Nakamoto's white paper [19] on an electronic cash system. Although the term "Blockchain" was fairly new, the bundled technology consisted of cryptography and hashing mechanisms that were explored long before the Blockchain [20].

The definition of Blockchain is that it is a technology of peer-to-peer (P2P) networking that uses block-type data structures as storage, consensus mechanisms to manage a shared distributed ledger, and encryption to ensure security during data transmission [21].

Figure 3 illustrates an overview of Blockchain anatomy. Distributed ledger technology (DLT) includes a validated record of transactions in the form of blocks that contain a nonce value, transaction data, timestamp, and the previous block hash to form a chain, a Blockchain. This figure gives an overview of Blockchain architecture as a peer-to-peer (P2P) network. It is composed of a set of miners having each a copy of the Blockchain. A new block is added after the mining process, which is validated by at least by 51% of the miners. This makes Blockchain one of the most important systems in terms of protecting data integrity as well as transparency and availability.

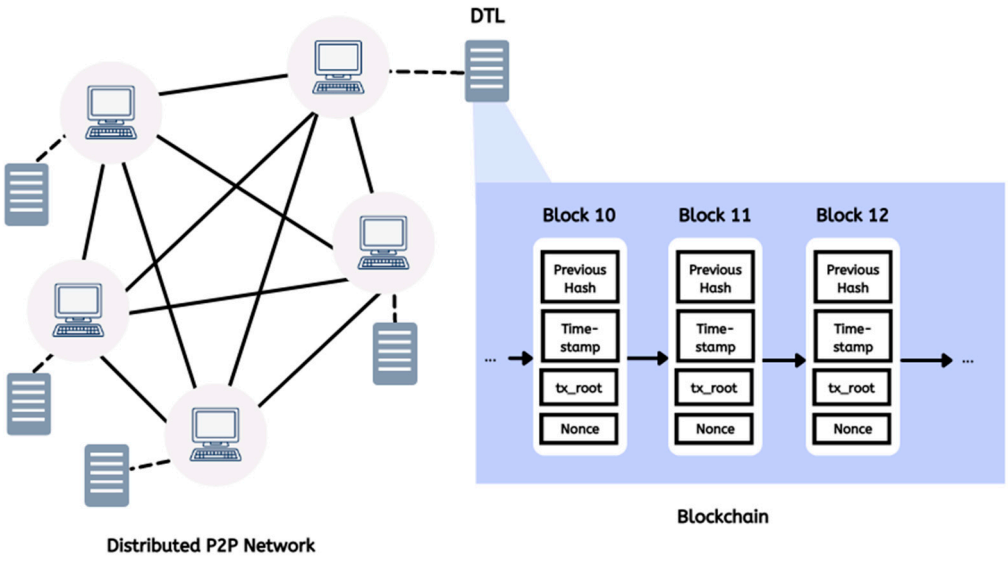

Figure 3. Blockchain as distributed DLT P2P technology.

3.2.1. Overview of Blockchain

Blockchain started with the first paper on Bitcoin in 2009 [19]. This era, the digital currency era, focused on developing decentralized-authority monetary transactional systems [22]. Next, research efforts was more focused on developing distributed applications (dApps) and the employment of smart contracts [21]. The use of artificial intelligence (AI) became integrated with Blockchain in order to be applied in industry 4.0 [23].

The type of Blockchain application is categorized based on its permissions as permissioned, permissionless, and federated Blockchain. Below, Table 4 summarizes the differences between these three types [24]. In fact, there are three type of Blockchain. The type of the Blockchain can be defined based on four characteristics, which are whether

the Blockchain is private or public and if it is controlled in a centralized or decentralized way. Two other characteristics that define the type of Blockchain are the level of security in addition to transaction speed and cost.

Table 4. Differences between permissionless, permissioned, and federated Blockchain [24].

	Permissionless	**Permissioned**	**Federated**
Publicity	Public	Private	Private
Authority	Decentralized	Centralized	Decentralized
Security	Less secure	Most secure	Secure
Transaction speed and cost	High	Less	Less

3.2.2. Components of Blockchain

Blockchain consists of multiple technology components which enable it to deliver the special characteristics of Blockchain, including security. There are six main Blockchain components which can be explained as follows:

1. Cryptographic hash function: Blockchain employs hashing in two ways, in the cryptographic challenge and in the Merkle tree. The cryptographic challenge, the nonce, is the value that miner nodes compete to calculate. On the other hand, the Merkle tree is the representation of the transactions as hashed values [24].
2. Asymmetric key encryption: Asymmetric encryption, or public-key encryption, is applied in addresses and digital signatures. The transactions are signed by the sender's private key, while the public key is used in the node's wallet address [24].
3. Transactions: A transaction is the exchange of transmits, processes, and storages of digital assets to control the state among the Blockchain nodes. Several transactions will create a block.
4. Consensus mechanisms: An agreement protocol to validate the new to-be-added block. Many consensus mechanisms exist. Table 5 shows a brief review of the four most used and well-known consensus algorithms.

Table 5. Summary of consensus algorithms.

Consensus Algorithms	**Steps**	**Blockchain**	**Remarks**
Proof of Work [21]	1. Transactions grouped into memory pool (mempool). 2. Miners try to solve the cryptographic challenge to validate. 3. The winner, the first to solve the challenge, is rewarded. 4. Others verify the proof. A block (mempool) is attached.	Public	First protocol in Blockchain [19]. High computational requirements. Less efficiency [23].
Proof of Stake [25]	1. Nodes, validators invest an amount of stake (monetary value) to participate. 2. Random validator is selected. 3. Validator approves the block, gets rewarded. 4. If the block is malicious, validator is deprived of their stake.	Public	More resource efficient [21]. The selection is not that "random". The higher a validator invests, the higher chance of being chosen [24].

Table 5. *Cont.*

Consensus Algorithms	Steps	Blockchain	Remarks
Proof of Elapsed Time [21]	1. Nodes wait for a random time. 2. After waiting, nodes become idle for a specific time. 3. The first to become active wins the block validation.	Private	System clock can be compromised [24].
Practical Byzantine Fault Tolerance	1. A generator is chosen to collect and choose the block signors. 2. Signors use their digital signature to validate block integrity. 3. If the fault is f, $2f + 1$ of $3f + 1$ must reach a consensus.	Private	Addresses the scalability issues [21].

In the following table, we discuss four consensus algorithms, starting with proof of work (PoW), which was first used with Bitcoin. The Proof of Stake (PoS) was proposed to optimize the use of resources. The proof of elapsed time is a special type of consensus algorithm based on time. The fourth one is called practical Byzantine fault tolerance and addresses the scalability issues.

5. Smart contracts: It is a program that contains code and controls the state of the ledger through logic execution; if the conditions are met, the logic is invoked [26].
6. Ledger: The ledger contains the validated blocks and group of transactions. Others refer to it as the Blockchain memory [24].

3.2.3. Characteristics of Blockchain

In this subsection, we give essential characteristics of Blockchains. The properties are the decentralization behavior, transparency, immutability and traceability, trusting, and anonymity. The numerous Blockchain components enable it to possess the following features [21,26]:

- Decentralization: where the ledger is shared among all the P2P network nodes.
- Transparency: where the ledger records are retrievable by any Blockchain node.
- Immutability and traceability: Where each block points to its predecessor, meaning a change to one block's content will not go unnoticed. Furthermore, where each block is timestamped to enhance the data traceability.
- De-Trusting: where no central authority or a third party is required to review the operations.
- Anonymity: where nodes are identified by their digital signature.
- Credibility: where internal calculations are automatically performed without human intervention, making Blockchain credible to perform secure operations.

3.3. Taxonomy of Federated Learning, Blockchain, and IoT

The integration of these two powerful technologies has many applications. Deploying Blockchain and federated learning integration in the IoT with all its different environments has become the main direction of authors and researchers [12]. Figure 4 illustrates the basic taxonomy of all layers of these technologies [10]. The Blockchain technology is foreseen to create a revolution in both industry and commerce, making great global economic changes, as it is immutable, transparent, and redefines trust, offering secure, fast, reliable, and transparent solutions. The IoT can leverage the absence of intermediates in the Blockchain, enabling users to communicate directly with IoT devices with no one intercepting them, which could offer a huge application area [27]. The following four layers of architecture can describe the general framework to develop application- and solution-merging between IoT, FL, and Blockchain. The IoT is responsible for data collection. The AI process is applied

through FL for privacy-preservation issues in case of sensitive data such as patient data. The aggregation, finally, is performed in the Blockchain as a trusted and confident layer.

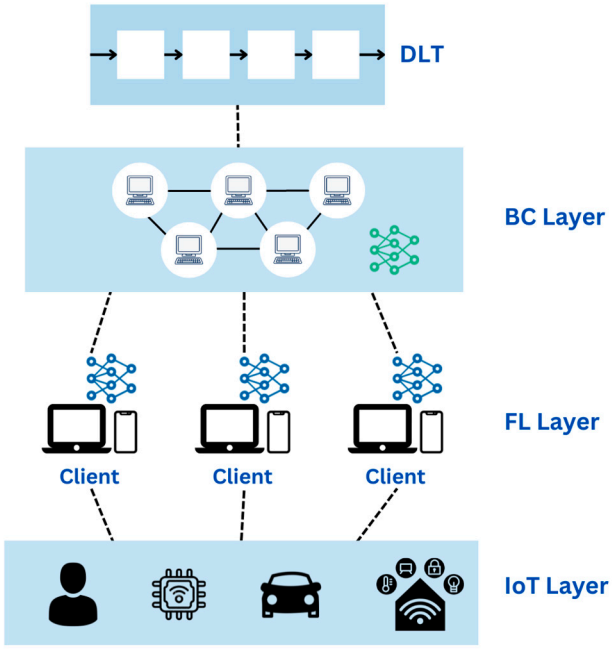

Figure 4. Taxonomy of federated learning, Blockchain, and IoT.

This integration between federated learning and Blockchain in the IoT could be shaped differently according to the type of application. Researchers of [18] provided a clear explanation of this integration's different architectures. However, it is out of this paper's scope.

4. Privacy and Security Challenges

The literature of federated learning is focused on developing ways that protect the privacy of data by only sharing the training gradients among nodes instead of the actual dataset [18]. Although strong noise addition techniques prevent some privacy attacks, the security of federated learning still lacks means of security. With its strong technologies, Blockchain integration with federated learning addresses many security concerns [12]. Attacks of tampering with the model by altering its gradients or poisoning the training dataset are still present in such integration.

4.1. Privacy Challenges

In the integration of Blockchain and federated learning in IoT, many privacy issues should be considered. Such challenges can be briefly explained as follows:

1. Shared data (P1): Blockchain storage capacity is limited, which means it could be a challenge to manage the storage of the massive shared raw data [10].
2. Model gradients leakage (P2): Can be referred to as message spoofing, which is when an adversary manages to obtain shared model gradients and, in time, derive information about the training data [28].
3. Linking attack (P3): The DLT enables connected nodes to have complete access to the transaction logs. An adversary could apply linking algorithms and extract information from the federated learning procedures [12].

4.2. Security Challenges

From a security perspective, it is a challenge to preserve trusted client participation. We focus on two main types of poisoning attacks that could happen in this environment to force the model to misclassify, which can be explained as follows [28]:

1. Data poisoning (S1), or poisoning attacks: when the adversary adds specific noise to the dataset or alters its labels, better known as label-flipping attacks.
2. Model poisoning (S2): similar to data poisoning, model poisoning is when the adversary tries to actively alter the model updates to change the model decision outcome.

5. Existing Solutions

Several researchers have focused on developing and finding ways that protect against poisoning attacks in a Blockchain, federated learning, and IoT-integrated ecosystem. Most solutions focused on finding a way to control the addition of new learning parameters. In the found research, solutions can be categorized into two main segments, reputation-based and noise-based.

A reputation-based integration controls new additions by controlling learners' participation. This control is based on their previous activities by assigning scores based on their participation quality. On the other hand, a noise-based integration controls additions by adding specific data to the new data submissions. The rest of this section discusses solutions existing in both categories.

5.1. Reputation-Based

Researchers in this area focused on finding a way to vouch for a learner node's legitimacy. One integration is in the work of [29], where the authors proposed a system of federated learning that analyzes people's readings of the late COVID-19 virus to classify and detect infected persons. They relied on Blockchain to use smart contracts and consensus mechanisms to calculate the scores and reputation for each participating edge device. In addition, the system uses Blockchain and smart contracts as provenance providers to limit the access to storage records. The proposed federated learning scheme achieved an accuracy of 90% in training and 85% in testing. Performance-wise, the edge devices have high and moderate energy consumption levels. This is because of the live model gradients sending and applying heavy encryption algorithms.

Similarly, the work of [30] has also relied on the worker, or learner, node reputation. Researchers proposed a reputation technique that identifies a malicious worker. This technique aggregates reputation from the other workers to decide that worker's legitimacy. A malicious worker would train wrongful data to propagate false updates to the global model, where these updates would affect that model's performance. However, they follow a framework of reputation that allows the task publisher to select a worker based on their reputation. Their experiment was with a 10-node network, which included two malicious workers. The lowest training accuracy was 76.12%, with two malicious workers and an attack strength of 0.9 out of 1.0. Their proposed framework achieved slightly better results than other trust-reputation-based frameworks.

Moreover, the work of [31] implemented federated learning into Blockchain to collaboratively train a traffic flow prediction (TFP) system of a neural network (NN) learning model. The authors designed a system to preserve vehicle update privacy and protect against poison attacks. This system relied on a consensus algorithm based on a delegated Byzantine fault tolerance (dBFT) protocol to determine low-quality or negative model updates. The proposed system performed well in poisoning attack prevention. The attack success rate (ASR) stayed under 10% with integrated federated learning compared to over 25% in unintegrated federated learning with 10%, 20%, and 30% malicious vehicles.

Authors of [32] proposed yet another reputation-based framework called TrustFed. The authors designed TrustFed to allow IoT devices to collaboratively train a global model based on cross-device federated learning (CDFL) schemes and Blockchain. The federated learning training was performed off-chain; data storage was also off-chain through Inter-Planetary File System (IPFS). More importantly, TrustFed's smart contract integration used three smart contracts: incentive, aggregator, and reputation. The incentive is to reward miners who contribute to validating the model updates. The aggregator is to choose the

central server at each learning round. Lastly, the reputation smart contract measures the reputation of participating nodes, thus avoiding malicious device participation.

TrustFed relied on off-chain and on-chain processes to determine the reputation scores of each participating node. Off-chain procedures include statistical analysis to detect outliers' updates at each learning round. On-chain procedures include aggregating trust scores where the device trust score is either incremented or decremented by 100 based on the latest fair training performance.

Experimenting on actual sensors' reading data showed that outlier detection (with worker nodes' reputation) achieved much better learning results. Malicious workers' updates were defined and removed from the next iteration, so aggregator loss was lower each time. Adding more workers to the learning task meant more transactions, creating communication overhead. However, the authors claim it was much less than transmitting raw data.

Authors of [33] proposed a fine-grained Blockchain-based federated learning framework for mobile edge computing systems. Their main contribution is to provide a reputation-based learning procedure to ensure honest and fair training participants. The suggested reputation system allows edge devices, fog nodes, and cloud servers to rate each other's effectiveness, activeness, and honesty through the use of dApps and reputation-based consensus mechanisms applied by smart contracts.

Moreover, the authors of [34] proposed a framework to secure the IoT infrastructure of federated learning with Blockchain. The trust-based flexible model used reinforcement learning. The process of choosing the participants in the learning process will be based on the trust score, and the evaluation process will be in a simulation using MATLAB.

The authors tested the model using a simulation compared to a direct trust model in terms of accuracy and detection rates, energy consumption, and network throughput. The proposed model showed high results with an accuracy value of approximately 0.93 and an approximately 0.96 detection rate. In terms of network, the proposed model has a higher bandwidth than the direct trust model with an average difference of approximately 100 Mbps and 2 s less in network latency. The proposed model performs better in energy consumption, with approximately 35% less energy consumed.

More recent work by [35] was also based on the Multi-Krum scheme. The authors proposed a commercial model where customers can participate in training a shared conventional neural network (CNN) model in a mobile edge computing (MEC) environment. The differential privacy (DP) protected the model gradients, where IPFS acted as the primary storage. They used the Algorand protocol as the consensus mechanism to promote a temporary leader that is responsible for aggregating the global model. Before the aggregation, the Multi-Krum scheme is applied.

The authors of [35] apply a reputation calculation to prevent malicious nodes' participation. When the participating nodes' updates prove legitimate, with using the Multi-Krum scheme, the nodes' reputation increases. Non-participating nodes that obtain a value of 0 reputation will not be allowed to be elected to train the model. Their experiment on the MNIST dataset proved to achieve an accuracy of 97%.

5.2. Noise-Based

Instead of calculating trust scores based on the worker node's contribution, other works added well-defined noise on the model updates to detect malicious model updates. For instance, authors of [36] proposed a framework to train an ML model using Blockchain-based federated learning in 5G networks. The framework divides the process into three main phases: initialization, aggregation, and updating. A task publisher node initiates a training task by sending the testing dataset, initial model, evaluation criteria (accuracy), and reward (monetary). Aggregation includes nodes training ML models locally, evaluating them to meet training criteria, and adding well-defined noise to protect the ML gradient's privacy. The updating includes the central server evaluating the updates and aggregating them to update the global model and send it to the publisher. A node is rewarded when it

achieves the accuracy threshold or higher. During experiments, the more the threshold for privacy increases, the more the accuracy decreases. However, adding more participants (p = 300) achieved higher accuracy results.

In [37], the authors illustrated a use-case of a smart healthcare system that uses federated learning and Blockchain in Medical IoT (mIoT) devices. In their paper, they addressed the privacy of patients' records by using an adaptive DF technique that adds noise to training gradients. To defend against poisoning attacks, the authors proposed a consensus protocol that identifies poisoned gradients through a verification committee.

The proposed mechanism acknowledged a slight performance accuracy loss despite preserving higher privacy in the results. From a performance perspective, the proposed system is slower than regular federated learning since it applies consensus algorithms. Their proposed system of detecting poison attacks performed well, keeping the attack success rate lower than 20% compared to over 50% in the regular FL.

Moreover, authors of [38] proposed Biscotti, a framework for Blockchain-based federated learning. The choice of peers at the learning round in Biscotti relied on the proof of federation (PoF) consensus algorithm to coordinate collaborative learning among the peers. Similar to the works of [35], to prevent poisoning attacks, they used a Byzantine tolerance aggregation scheme called Multi-Krum, which validates the peer model update by comparing it with other peers and measuring the noise difference. Noisier nodes are responsible for adding noise to model updates to prevent privacy leakages and help detect poisonous attacks.

With 30% of malicious nodes, the Biscotti test error was low compared to regular federated learning. At training, and with 200 nodes, as the time increased, the training error rates were kept low. However, if the malicious nodes were 50% of the participating nodes or more, the attacker could easily alter the global model outcome.

Like Biscotti, The authors designed BAFL [39] as a novel Blockchain-based asynchronous federated learning framework. BAFL controlled the updates of the global and local models of devices by identifying entropy noise values. The design of BAFL was to overcome regular synchronous federated learning, such as FLAvg, which usually could cause significant performance delays. BAFL has two main layers, the device layers (D) and the miners' layer (M). At each learning epoch, a miner randomly connects to a device. A device loads the global model and locally trains it. The device uploads the training parameters, including the time duration of one training round. The miner verifies the device update with the global model before adding it to the Blockchain. To detect poisoning attacks that could tamper with the model's parameters, BAFL used entropy noise to measure the authenticity of each device.

BAFL has achieved lower resource consumption and delay during experiments than the original synchronous AvgFL framework. In addition, BAFL also improved learning precision by 12.1%. To evaluate the poisoning attack detection, they assumed that 10 of 50 devices, or about 20% of participating nodes, were controlled by an attacker. BAFL proved its resilience against such attacks. However, similar to Biscotti [38], if the attacker had control of over 50% of the devices, that attacker could easily poison the global model.

5.3. Other Solutions

Some work to protect the IoT Blockchain-based federated learning adoption against poisoned attacks followed slightly different approaches. For instance, the work of [40] relied on the learning model accuracy to detect if there had been an attack attempt. The authors developed a mechanism comparing a new parameter update with known good model accuracy. If the parameter update degrades the model accuracy, the aggregator discards the update from aggregation. Their algorithm performed very well against 10%, 20%, and 30% of adversaries with very low accuracy degradation in the first round. However, as the number of rounds increases, the accuracy is not affected since malicious node updates are easily verifiable with good updates.

Other works relied on time to prove one update's legitimacy. For instance, authors of [41] provided the block-FL framework to enhance data privacy while maintaining trustful collaborative learning with Blockchain and federated learning. Block-FL uses a decentralized hash table (DHT) to only store the hash of the data source on-chain while keeping the data off-chain. As usual, the federated learning process is an aggregation process used to update the global model after verifying local model updates by miners. For poisoning attack resilience analysis, they assumed that a malicious attacker would try to replace the global model with their poisoned model. To prevent such an attack, Block-FL follows a mechanism of evaluating the computation time proportionality with data size.

Block-FL proved that the hash rate for an adversary to make turbulence on the ledger record is the lowest compared to federated learning and regular Blockchain. At the same time, the successful attack hash-rate requirement increases as the number of added blocks increases, which makes poisoning attacks even harder.

A similar work by [42] recently provided a data-driven cognitive computing (D2C) framework based on Blockchain-enabled federated learning. The authors' main drive was to overcome the issues faced by industry 4.0 devices, such as privacy leakage. For the data, they chose to store the hashes only, instead of the whole data, using the DHT. For verification, the framework relied on consensus and intensive mechanisms using PoW and two types of incentives, token reward and data reward. The token reward was for miners, while the data reward was for end devices.

The authors used proof of elapsed time (PoET) to spot poisonous model updates to verify the computation time with the data sample size. At each learning round, a temporary central server was chosen, an aggregator. Choosing an aggregator was based on the two-player game of the Markov decision process (MPC) between an aggregator and an adversary. Similar to [36], the hash-rate requirement increased as the number of blocks increased, making it harder for an adversary. However, there was still convergence latency in block generation time.

Others used consensus mechanisms to protect data from leakage [42,43]. For instance, authors of [42] applied federated learning on a permissioned Blockchain in an iIoT environment. In such a sensitive environment, data privacy and security matter the most. The authors proposed a scheme that follows federated learning aggregation procedures while verifying data provider nodes to prevent leakage. A data-sharing request goes through a proof of quality (PoQ) consensus mechanism to verify the data from each data provider node. The proposed scheme achieved good results with above 0.9 accuracies. However, increasing the number of data providers meant a degradation in both time and accuracy performance.

Most federated learning with Blockchain integrations were with the iIoT infrastructure. Works of [44–46] primarily focused on applying privacy measures, designing an auditable record of transactions, and eliminating the central aggregation server of federated learning in their Blockchain integration. In [45], the authors designed a system that detects iIoT device failure. They used the Merkle tree to anchor gathered devices' data to the Blockchain, and they used smart contracts to apply an incentive mechanism to reward training participating nodes with tokens.

Moreover, ref. [45] proposed a similar use of federated learning and Blockchain in iIoT. In that work, the authors focused on how to preserve communication costs. The proposed mechanism applied CNN and used a k-top algorithm to limit the training gradients of one trainee node before the local aggregation. This mechanism applies Gaussian noise to protect the privacy of the model gradients that are stored on-chain. In [46], the authors applied differential privacy on data by using homomorphic encryption. Using LaPlace and Pillar, cryptosystems encrypted the data to train it with K-means, random forest, and AdaBoost. Lastly, the global model gradients were stored on-chain after aggregation. However, the works of [44–46] did not provide ways to prevent poisonous node additions.

Others had a somewhat separate deployment of federated learning with Blockchain [47–50]. Claiming to be the first application of federated learning with Blockchain in an intrusion detection system (IDS), the authors of [47] used MultiChain permissioned Blockchain to

ensure the training epoch data integrity. The usage of MultiChain gained the proposed system the ability to store the data of the training round and organize the next round's leader. During experiments, the proposed system performed well. However, with 12 deep learning servers, there was an executional delay compared with regular Blockchain, by 5–15%.

Authors of [48] proposed a framework that leverages federated learning and Blockchain in the Internet of Battle Things (IoBT). The edge-computing-based system consists of four layers: data, edge, fog, and cloud layers. Data is where the data collection happens, the edge is where the model training and off-chain aggregation happens, fog follows a similar pattern, while the cloud layer stores the final globally trained model.

An experiment to test the performance of [48]'s proposed system was conducted using an imagery dataset of airplanes, birds, drones, and ships. With two learning rate criteria of 0.01 and 0.02, the first setting of fixed participants achieved 92% and 94% in edge nodes, respectively, and 99% and 97% in fog nodes, respectively, over 50 rounds of learning. In contrast, a second set of randomly selected participants achieved 89% and 92% in edge nodes, respectively, and 97% and 96% in fog nodes, respectively. While it is lesser than fog nodes, it is still regarded as having high accuracy with low loss.

The work of [50] is another example of another semi-separate application in anomaly detection systems. The authors designed an asynchronous learning system to detect anomalies in an IoT system. Using Blockchain to validate the model updates enhanced privacy and security.

Works of [49,51] used Blockchain as an authentication authority to provide the required access and participation. In [49], authors deployed a real-time data-processing and multi-agent system in an Internet of Medical Things (IoMT) environment. The authors employed three agents: learning agent, data management agent, and indirect agent. They used separate cloud storage to store the datasets of patients and the classifier models. Similar, but in a different flavor, [51] uses federated transfer learning (FTL) for each iIoT-device-trained parameter's transfer to a cloud server for aggregation. The consensus mechanism was Ripple, where a device must be approved by 51% of connected nodes to be authenticated.

The paper of [52] proposed a multi-layer consensus system for the Internet of Vehicles, yet another flavor of IoT. The Blockchain-enabled hierarchal mechanism relied on a proof of knowledge (PoK) consensus mechanism at two layers with roadside units (RSU) and vehicles. The first layer was the ground chains (GC) layer, where vehicles collected data from surrounding areas that were considered as federated learning training sets. The second layer was the top chain (TC). The RSUs will also participated in the federated learning process by collecting data from their surrounding areas, merging their results with the transaction results from GC nodes, and uploading them to the chain.

The PoK of [52] rewards higher accuracy workers with higher amounts, which will also work as an incentive mechanism. Dishonest workers are identified through a validation process of their achieved accuracy by the leader node. The proposed system achieved a result that was 10% higher compared with regular consortium Blockchain.

Most of the found adoptions of federated learning with Blockchain did not address poisoning attack prevention. The authors of [53] suggested a model for market trading of resources in decentralized edge companies. In terms of privacy, they included federated learning that depends on requesting training models between companies instead of requesting raw data to prevent any possible leakage while fulfilling the requester's needs.

Table 6 below summarizes the found literature by highlighting the integration scope and analyzing how they mitigate the previously mentioned privacy and security challenges.

Table 6. Summary of existing solutions of federated learning and Blockchain in IoT.

Type	Ref.	Consensus	Application	Integration Scope [1]					Privacy and Security [2]			
				Con.	Incent.	Prov.	IPFS	P1gol	P2	P3	S1	S2
Reputation-Based	[29]	-	IoHT	√	-	√	-	√	√	-	-	√
	[30]	BFTP	Mobile network	√	-	-	-	-	√	-	√	√
	[31]	dBFTP	IoV	√	-	-	-	√	√	√	√	-
	[32]	-	iIoT	√	-	-	√	√	-	-	√	√
	[33]	-	Edge computing	-	√	√	√	-	√	-	-	√
	[34]	BFTP	IoT infrastructure	√	√	-	-	√	√	-	-	√
	[35]	Algorand	Edge computing	√	-	-	√	√	√	-	-	√
Noise-Based	[36]	-	Mobile network	-	√	-	-	-	√	√	-	√
	[37]	Algorand	mIoT	√	-	-	-	-	√	-	-	√
	[38]	PoF	Edge computing	√	-	-	-	-	√	√	-	√
	[39]	PoW	Edge computing	√	√	-	-	-	√	-	√	√
Other	[40]	-	Edge computing	√	-	-	-	-	√	-	-	√
	[41]	PoW	Fog computing	√	-	-	-	√	√	-	√	√
	[54]	PoW and PoET	Industry network	√	√	-	-	√	√	√	-	√
	[42]	-	IoV	-	-	-	√	-	√	-	-	-
	[43]	PoQ	iIoT	√	-	√	-	√	-	-	√	-
	[44]	PoW	iIoT	-	√	-	-	√	-	-	√	-
	[45]	-	iIoT	√	-	-	-	-	√	-	-	-
	[46]	RAFT	iIoT	√	-	-	-	-	√	-	√	√
	[47]	Round Robin	IoT	√	-	-	-	-	-	-	-	√
	[48]	-	IoBT	-	-	-	-	-	√	-	-	√
	[49]	-	IoMT	-	-	-	-	√	-	-	√	-
	[50]	-	IoT infrastructure	-	-	-	-	-	√	-	-	-
	[51]	Ripple	iIoT	√	-	√	-	√	-	-	-	-
	[52]	PoK	IoV	√	√	-	-	√	-	-	√	-
	[53]	PoW	Edge computing	√	√	√	-	√	-	-	-	√

[1] A summary of the solution with regard to federated learning with Blockchain integration scope by consensus protocols, incentive protocols, Blockchain as provenance provider, and usage of IPFS. [2] To measure if the proposed solution resolution considered security and privacy challenges.

In this table, we compare relevant research works that used Blockchain and federated learning in the IoT ecosystem aiming to protect the privacy of client data. We arrange the table into six principles columns. The first column indicates the type of method which can be based on reputation, noise, or other. The second column indicates the reference itself. The third column refers to the applied consensus. The fourth column indicates the origin of data, which can be health data, from a mobile network, IoV data, iIoT data, edge data, or fog data. The column before the last summarizes the integration scope by consensus protocols, incentive protocols, Blockchain as provenance provider, and usage of IPFS. The last column focuses on privacy and security, aiming to measure if the proposed solution resolution considered security and privacy challenges.

5.4. Lessons Learned

After the review of numerous works that included variations of federated learning and Blockchain in the IoT environment, the following points summarize existing solutions:

- Most of the found work focuses on applying federated learning with Blockchain with a disregard to applying methods to detect poisonous attacks.
- We found that most work is reputation-based rather than noise-based to prevent the occurrence of poisonous attacks.
- The application scope of federated learning and Blockchain integration heavily focused on industrial, medical, and communications area.

6. Conclusions and Future Directions

This paper presented a review of two leading technologies that are leveraged to enhance security and privacy. IoT devices applications include the sharing of massive raw data. Federated learning is integrated to provide intelligence to these low-level devices while preserving the privacy of data by only sharing the trained model. Traditional federated learning is centralized and suffers from security issues of untrusted clients. The added layer of Blockchain integration resolved multiple issues of trust and security.

This paper reviewed the taxonomy of such integration while briefly describing the elements of each technology. After that, this paper discussed five main security and privacy concerns that the integration of federated learning, Blockchain, and IoT faces. By reviewing the existing literature, this paper compared and measured the integration scope and security and privacy considerations.

For future work, this survey concludes that the number of existing solutions that address poisoning attacks threats in federated learning and Blockchain integration is still scarce. Although federated learning is designed to protect the privacy of training data, there is still a need to guarantee the security and privacy of the training data. More work needs to be done to address issues of computational and resources limitation in edge devices. There are few existing solutions to address protection against dishonest participants' attempts to poison and alter the shared training process. This paper aims to encourage future work to enhance the security and privacy of both technologies in an IoT environment.

Our basic aim when preparing this paper was to propose a short and accurate survey that focuses on the most relevant research work in IoT ecosystem data privacy preservation based on joining Blockchain to federated learning. We were motivated by regulations restricting data sharing and privacy concerns. The use of IT solutions in healthcare saves lives but also leads to several problems related, in particular, to the security aspect. Indeed, the poisoning of datasets as well as the falsification of decisions can cause false diagnoses affecting human life. This makes the execution protection of learning models sometimes more important than improving the techniques themselves. We believe that our paper will serve as a key reference for researchers interested in improving solutions based on mixing Blockchain and federated learning in IoT environments while preserving privacy. In the future, the tradeoff between Blockchain cost and the index of privacy preservation may be a hot topic of research. Certainly, a partial amount of data can be shared, and this will affect positively the output of machine-learning-based applications. Another improvement can

focus on the clustering of FL clients who can share their data before the final aggregation with others.

Author Contributions: Conceptualization, M.A.A. and T.M.; methodology, M.A.A.; investigation, M.A.A.; resources, M.A.A.; data curation, M.A.A.; writing—original draft preparation, M.A.A.; writing—review and editing, T.M.; visualization, T.M.; supervision, T.M.; project administration, T.M.; funding acquisition, T.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Qassim University, represented by the Deanship of Scientific Research, grant number COC-2022-1-1-J-26046.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The author(s) gratefully acknowledge Qassim University, represented by the Deanship of Scientific Research, on the financial support for this research under the number (COC-2022-1-1-J-26046) during the academic year 1444 AH/ 2022 AD.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
2. Vailshery, L. IoT Connected Devices Worldwide 2019–2030. Statista. Available online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 15 October 2022).
3. *The Internet of Things Reference Model*; CISCO: San Jose, CA, USA, 2014. Available online: https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf (accessed on 10 October 2022).
4. Mukherjee, M.; Matam, R.; Mavromoustakis, C.X.; Jiang, H.; Mastorakis, G.; Guo, M. Intelligent edge computing: Security and privacy challenges. *IEEE Commun. Mag.* **2020**, *58*, 26–31. [CrossRef]
5. Ghaznavi, M.; Jalalpour, E.; Salahuddin, M.A.; Boutaba, R.; Migault, D.; Preda, S. Content delivery network security: A survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2166–2190. [CrossRef]
6. Murshed, M.G.S.; Murphy, C.; Hou, D.; Khan, N.; Ananthanarayanan, G.; Hussain, F. Machine Learning at the Network Edge: A Survey. *ACM Comput. Surv.* **2021**, *54*, 170. [CrossRef]
7. Konečný, J.; McMahan, H.B.; Yu, F.X.; Richtárik, P.; Suresh, A.T.; Bacon, D. Federated Learning: Strategies for Improving Communication Efficiency. *arXiv* **2017**, arXiv: 1610.05492. [CrossRef]
8. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Poor, H.V. Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1622–1658. [CrossRef]
9. Gad, A.G.; Mosa, D.T.; Abualigah, L.; Abohany, A.A. Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 6719–6742. [CrossRef]
10. Wang, Z.; Hu, Q. Blockchain-based Federated Learning: A Comprehensive Survey. *arXiv* **2021**, arXiv: 2110.02182. [CrossRef]
11. Qammar, A.; Karim, A.; Ning, H.; Ding, J. Securing federated learning with blockchain: A systematic literature review. *Artif. Intell. Rev.* **2022**, *56*, 3951–3985. [CrossRef]
12. Ali, M.; Karimipour, H.; Tariq, M. Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Comput. Secur.* **2021**, *108*, 102355. [CrossRef]
13. Issa, W.; Moustafa, N.; Turnbull, B.; Sohrabi, N.; Tari, Z. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Comput. Surv.* **2023**, *55*, 1–43. [CrossRef]
14. Wang, N.; Yang, W.; Wang, X.; Wu, L.; Guan, Z.; Du, X.; Guizani, M. A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles. *Digit. Commun. Netw.* **2022**. [CrossRef]
15. Javed, A.R.; Hassan, M.A.; Shahzad, F.; Ahmed, W.; Singh, S.; Baker, T.; Gadekallu, T.R. Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey. *Sensors* **2022**, *22*, 4394. [CrossRef] [PubMed]
16. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Syst.* **2023**, *40*, e13103. [CrossRef]
17. McMahan, H.B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication-Efficient Learning of Deep Networks from Decentralized Data. *arXiv* **2017**. [CrossRef]
18. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated Machine Learning: Concept and Applications. *arXiv* **2019**. [CrossRef]
19. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. p. 9. Available online: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (accessed on 28 October 2022).
20. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]

21. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The Revolution of Blockchain: State-of-the-Art and Research Challenges. *Arch. Comput. Methods Eng.* **2021**, *28*, 1497–1515. [CrossRef]
22. Efanov, D.; Roschin, P. The All-Pervasiveness of the Blockchain Technology. *Procedia Comput. Sci.* **2018**, *123*, 116–121. [CrossRef]
23. Cummings, S. The Four Blockchain Generations. The Capital. 2 February 2019. Available online: https://medium.com/the-capital/the-four-blockchain-generations-5627ef666f3b (accessed on 22 November 2022).
24. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; NIST Internal or Interagency Report (NISTIR) 8202; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2018. [CrossRef]
25. Proof-of-Stake (PoS). Ethereum.Org. Available online: https://ethereum.org (accessed on 23 November 2022).
26. Lu, Y. The blockchain: State-of-the-art and research challenges. *J. Ind. Inf. Integr.* **2019**, *15*, 80–90. [CrossRef]
27. Alfrhan, A.; Moulahi, T.; Alabdulatif, A. Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT). *Blockchain Res. Appl.* **2021**, *2*, 100036. [CrossRef]
28. Liu, P.; Xu, X.; Wang, W. Threats, attacks and defenses to federated learning: Issues, taxonomy and perspectives. *Cybersecurity* **2022**, *5*, 4. [CrossRef]
29. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
30. Kang, J.; Xiong, Z.; Niyato, D.; Zou, Y.; Zhang, Y.; Guizani, M. Reliable Federated Learning for Mobile Networks. *IEEE Wirel. Commun.* **2020**, *27*, 72–80. [CrossRef]
31. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Gener. Comput. Syst.* **2021**, *117*, 328–337. [CrossRef]
32. ur Rehman, M.H.; Dirir, A.M.; Salah, K.; Damiani, E.; Svetinovic, D. TrustFed: A Framework for Fair and Trustworthy Cross-Device Federated Learning in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *17*, 8485–8494. [CrossRef]
33. ur Rehman, M.H.; Salah, K.; Damiani, E.; Svetinovic, D. Towards Blockchain-Based Reputation-Aware Federated Learning. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 183–188. [CrossRef]
34. Otoum, S.; Ridhawi, I.A.; Mouftah, H. Securing Critical IoT Infrastructures With Blockchain-Supported Federated Learning. *IEEE Internet Things J.* **2022**, *9*, 2592–2601. [CrossRef]
35. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 1817–1829. [CrossRef]
36. Liu, Y.; Peng, J.; Kang, J.; Iliyasu, A.M.; Niyato, D.; El-Latif, A.A.A. A Secure Federated Learning Framework for 5G Networks. *IEEE Wirel. Commun.* **2020**, *27*, 24–31. [CrossRef]
37. Chang, Y.; Fang, C.; Sun, W. A Blockchain-Based Federated Learning Method for Smart Healthcare. *Comput. Intell. Neurosci.* **2021**, *2021*, e4376418. [CrossRef] [PubMed]
38. Shayan, M.; Fung, C.; Yoon, C.J.M.; Beschastnikh, I. Biscotti: A Blockchain System for Private and Secure Federated Learning. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1513–1525. [CrossRef]
39. BAFL: A Blockchain-Based Asynchronous Federated Learning Framework. IEEE Journals & Magazine. IEEE Xplore. Available online: https://ieeexplore.ieee.org/abstract/document/9399813 (accessed on 30 October 2022).
40. Short, A.R.; Leligou, H.C.; Papoutsidakis, M.; Theocharis, E. Using Blockchain Technologies to Improve Security in Federated Learning Systems. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020. Available online: https://ieeexplore.ieee.org/abstract/document/9202584 (accessed on 24 October 2022).
41. Qu, Y.; Gao, L.; Luan, T.H.; Xiang, Y.; Yu, S.; Li, B.; Zheng, G. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. *IEEE Internet Things J.* **2020**, *7*, 5171–5183. [CrossRef]
42. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
43. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4177–4186. [CrossRef]
44. Zhang, W.; Lu, Q.; Yu, Q.; Li, Z.; Liu, Y.; Lo, S.K.; Chen, S.; Xu, X.; Zhu, L. Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT. *IEEE Internet Things J.* **2021**, *8*, 5926–5937. [CrossRef]
45. Zhang, X.; Hou, H.; Fang, Z.; Wang, Z. Industrial Internet Federated Learning Driven by IoT Equipment ID and Blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, e7705843. [CrossRef]
46. Jia, B.; Zhang, X.; Liu, J.; Zhang, Y.; Huang, K.; Liang, Y. Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4049–4058. [CrossRef]
47. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study. *Appl. Sci.* **2018**, *8*, 2663. [CrossRef]
48. Sharma, P.K.; Park, J.H.; Cho, K. Blockchain and federated learning-based distributed computing defence framework for sustainable society. *Sustain. Cities Soc.* **2020**, *59*, 102220. [CrossRef]
49. Połap, D.; Srivastava, G.; Yu, K. Agent architecture of an intelligent medical system based on federated learning and blockchain technology. *J. Inf. Secur. Appl.* **2021**, *58*, 102748. [CrossRef]

50. Cui, L.; Qu, Y.; Xie, G.; Zeng, D.; Li, R.; Shen, S.; Yu, S. Security and Privacy-Enhanced Federated Learning for Anomaly Detection in IoT Infrastructures. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3492–3500. [CrossRef]
51. Zhang, P.; Sun, H.; Situ, J.; Jiang, C.; Xie, D. Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing. *IEEE Access* **2021**, *9*, 98630–98638. [CrossRef]
52. Chai, H.; Leng, S.; Chen, Y.; Zhang, K. A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3975–3986. [CrossRef]
53. Fan, S.; Zhang, H.; Zeng, Y.; Cai, W. Hybrid Blockchain-Based Resource Trading System for Federated Learning in Edge Computing. *IEEE Internet Things J.* **2021**, *8*, 2252–2264. [CrossRef]
54. Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2964–2973. [CrossRef]