




Article

Blockchain Federated Learning for In-Home Health Monitoring

Komal Farooq¹, Hassan Jamil Syed^{1,2,*} , Samar Othman Alqahtani³, Wamda Nagmeldin³ ,
Ashraf Osman Ibrahim²  and Abdullah Gani⁴

¹ Department of Computer Science, National University Computer and Emerging Sciences, Karachi 75030, Pakistan

² Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, Kota Kinabalu 88400, Malaysia

³ Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, AL-Kharj 11942, Saudi Arabia

⁴ Department of Computer System & Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

* Correspondence: shjamil@ums.edu.my

Abstract: This research combines two emerging technologies, the IoT and blockchain, and investigates their potential and use in the healthcare sector. In healthcare, IoT technology can be utilized for purposes such as remotely monitoring patients' health. This paper details ongoing research towards individualized health monitoring using wearable gadgets. The goal of improving healthcare facilities and improvement of the quality of life of citizens naturally brings up Internet of Things (IoT) technologies for consideration. Health observation is exceptionally critical in terms of avoidance, especially since the early determination of illnesses can minimize trouble and treatment costs. The cornerstones of intelligent, integrated, and individualized healthcare are continuous monitoring of physical signs and evaluation of medical data. To build a more reliable and robust IoMT model, the study will monitor the application of blockchain technology in federated learning (FL). A viable way to address the heterogeneity problem in federated learning is to design the system, data, and model tiers to lessen heterogeneity and produce a high-quality, tailored model for each endpoint. Blockchain-based federated learning allows for smarter simulations, lower latency, and lower power consumption while maintaining privacy at the same time. This solution provides another immediate benefit: in addition to having a shared model upgrade, the updated model on phones will now be used automatically, giving personalized knowledge about the phone is used.

Keywords: blockchain; federated learning; health monitoring; Internet of Medical Things (IoMT); personalized healthcare



Citation: Farooq, K.; Syed, H.J.; Alqahtani, S.O.; Nagmeldin, W.; Ibrahim, A.O.; Gani, A. Blockchain Federated Learning for In-Home Health Monitoring. *Electronics* **2023**, *12*, 136. <https://doi.org/10.3390/electronics12010136>

Academic Editors: Wen Sun, Lexi Xu, Hui Xia and Libin Yang

Received: 10 November 2022

Revised: 19 December 2022

Accepted: 21 December 2022

Published: 28 December 2022



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The industry is moving away from a responsive to a constructive approach to health challenges in terms of earlier detection, mitigation, and protracted maintenance of health and wellness. Individual well-being monitoring and management must be prioritized to achieve these goals. When the objectives of delivering improved healthcare services and enhancing citizen quality of life are pursued, Internet of Medical Things (IoMT) technologies are considered. The creation, implementation, and upkeep of connected, intelligent, and personalized healthcare systems and services will heavily depend on them. These services can assist with ongoing physical condition monitoring and automatic processing. As a result, processed events are generated, which may show conditions such as high blood pressure, tension, etc. Wearable sensors are essential for continuously monitoring physical characteristics [1,2].

A network of portable medical devices called the “Internet of Medical Things” (IoMT) gathers medical data on a particular patient. These files are large and sensitive, and require a secure environment. As blockchain technology develops, researchers focus on using it to

bring cryptography to healthcare applications. The blockchain network has proven to be the most dependable and decentralized system. It offers intuitive interfaces such as tamper-proofing, immutability, traceability, data storage, confidentiality, and privacy without a third party's participation. Blockchain technology can prevent data from being manipulated and maintain data integrity, and can provide secure access, distributed computation, and decentralized data storage. In conclusion, in this paper, we describe a secure medical data processing and storage system that employs blockchain to safeguard client data privacy. Concerns about security and privacy have been addressed using federated learning [3–6].

Machine learning and blockchain technologies have been studied for possible medical uses, with only minor success. This combination is employed in federated learning and enables it to execute distant functions and analyses without transferring strictly guarded personal health information. The goal of ensuring better healthcare services and enhancing people's quality of life through IoT devices would lead us to accept IoMT technology. There is an increasing need for technological advancement that can assist with moving treatment from hospital-centered to home-centered care. To prevent data from being isolated and to secure the confidentiality and anonymity of IoMT data, federated learning (FL) has been proposed. Private IoMT data can then be educated on the owner's property. Blockchain is used for peer-to-peer communication. Blockchain helps non-trusting participants connect without the use of an intermediary.

By 2025, there will be 1.2 billion people who are 60 or older, and by 2050, there will be 2 billion. This prediction comes from the World Health Organization (WHO). Since the aging population tends to experience physical ailments, behavioral disorders, psychological disorders, and other co-morbidities at a higher frequency, issues such as a shortage of medical supplies and a drop in healthcare services arise. Additionally, some older persons (such as senior singles and elderly couples) choose to reside independently in their houses, which increases their risk of life-threatening falls and strokes. Older persons who frequently live alone in their homes, such as elderly couples or isolated individuals, are more likely to have potentially fatal mishaps and seizures. As a result, there is a growing demand for technological progress that can help shift the focus of elder care from hospitals to homes. With the prediction of 18 billion devices by 2022, the Internet of Things (IoT) has grown into a technology with significant effects across several vertical markets. The millions of small, reasonably priced devices are expected to lead to the availability of several IoT services on a global scale. In addition, many Internet of Things (IoT) devices have limited functionality, and IoT access control solutions now in use that rely on centralized, hierarchical systems present significant issues. Personalized Federated Learning allows smarter simulations, lower latency, and lower power consumption while at the same time maintaining privacy. This solution provides yet another immediate benefit: in addition to having a shared model upgrade, the updated model on the phone will now be used automatically, allowing individuals to gain personalized knowledge about how they use the phone [7]. Blockchain is a promising technique with a broad range of uses and sectors for greater security, privacy, and trust, thanks to its distinctive characteristic that makes it robust and unhackable. The security and confidentiality concerns with the IoT network can be resolved using the blockchain. On the contrary, the prospect of integrating and utilizing blockchain in IoT networks must be considered. The healthcare and medical industries can use the combination of IoT and blockchain to address present challenges, like drug provenance. The capabilities and reliability of the current healthcare business could be improved by combining these two powerful technologies [2,8,9].

Home health monitoring is the use of information technology to monitor patients' health through wearable devices in their homes to ensure that necessary action is taken. However, there are many significant obstacles facing wearable healthcare right now. One issue is that data commonly occurs as isolated islands in the real world. Although there is a ton of data in many organizations, institutions, and fields, it is not practical to interchange information because of privacy and security concerns. For example, if the same customer uses a product from two separate providers, his data is saved on two different clouds that

cannot be shared. As a result, it is difficult to develop effective models that utilize this important data.

The other important challenge is personalization, which refers to the personalization of wearable healthcare devices. Wearable technology refers to electronic devices worn on the patient's body, such as on the wrist, arm, or head. Healthcare devices are expected to meet a growing demand for remote medical services that are not constrained by space or time, as well as a growth in demand for medical services among the elderly, who have limited mobility and access to professional medical services. It is critical to identify the factors that influence a person's motivation to use healthcare wearable technology indefinitely. Physical features and daily activity routines vary amongst users. As a result, the common approach fails to provide personalized healthcare.

The wide area of the IoT has enabled network connectivity in homes, automobiles, and even cities. However, due to their limited capabilities, IoT devices have not been utilized to trigger emergency alerts directly to healthcare providers during an emergency.

Lastly, blockchain technology can prevent data manipulation, maintain data integrity, and provide secure access, distributed computation, and decentralized data storage.

This research aims to address wearable medical devices' personalization and security concerns. The accompanying set of goals must be met for this research's goal to be accomplished. We can conclude that the objectives of this study are as follows:

- To review the most advanced blockchain federated learning and pinpoint the main issue with the existing blockchain FL.
- To investigate and analyze the Blockchain Technology solution.
- To evaluate the proposed blockchain solution and verify it by comparing it with existing solutions.

Machine learning and blockchain technologies have been studied for possible medical uses, with only minor success. This combination is employed in federated learning, which makes it easier to execute distant functions and analyses without transferring strictly guarded personal health information. Wearable technology, such as smartphones and wristbands, has quickly advanced, making it easier to learn about people's health, including their movements, relaxation, athletics, and other behaviors.

Blockchain offers a safe and decentralized method of data sharing. It is a method of information preservation that makes it challenging or impossible to change, hack, or deceive the device. The most stable and decentralized system so far has been the blockchain network. It offers intuitive interfaces such as tamper-proofing, immutability, traceability, data storage, confidentiality, and privacy without third-party involvement [7]. Blockchain-based federated learning allows for smarter simulations, lower latency, and lower power consumption while at the same time maintaining privacy.

The contributions of this paper are as follows:

- Reviewed the state-of-the-art Blockchain Federated Learning to pinpoint the main issue with the existing solutions.
- Collected data using wearable IoT.
- Developed an automated system that analyzes patients' live data.
- Proposed a framework based on blockchain to provide privacy preservation mechanisms to improve the system's privacy.
- The FL algorithm, which encourages on-device machine learning through decentralized learning.

The rest of this paper is organized as follows: Section 2 provides related work. Section 3 introduces the methodology. Section 4 describes the proposed framework. Section 5 discusses the results obtained. Section 6 presents some open issues.

2. Related Work

This section comprehensively reviews the state-of-the-art blockchain federated learning solutions for IoT devices. While federal learning (FL) can implement distributed

training machine learning models over numerous devices while maintaining data privacy, significant flaws remain, such as single-point failure and a lack of motivation. As a distributed ledger, blockchain may be used to create a novel FL architecture to handle such challenges.

Many researchers have studied the application's privacy and security in the available literature. However, there is still a shortage of exploratory studies and review work on the function of blockchain in FL.

The goal of [7] was to create a smart health monitoring system. Since each individual's health data involves privacy, there was a risk of privacy leakage. In addition, real-time data was required for some emergencies without interruption over the internet. It was not possible to integrate the health data of multiple users for machine learning model training. Federated Learning was developed to address this issue by allowing devices to learn a model without sharing data or revealing any personal information. FedHome was presented, which is a cloud-edge-based framework. It is a component of the generative convolutional autoencoder design that aids in reducing the uneven and non-IID distribution of user input. Numerous studies utilizing the Human Activity dataset showed that FedHome reaches 95.41% accuracy, but not all clients receive high accuracy from FedHome. Some users may perform poorly in a global network built through federated learning. In the same scenario, two clients can have two different accuracy rates.

Qiong et al. [7] looked into major heterogeneity issues in the IoT environment. They implemented personalization at the device, data, and model levels to attenuate heterogeneities and establish a customized model for each device to address concerns with devices, models, and statistical heterogeneity.

Federated meta-learning is used to resolve statistical heterogeneity through the FedAvg algorithm. Federated multi-task learning is used to resolve model heterogeneity. The PerFit framework was proposed for intelligent IoT applications and resolved heterogeneity issues, but its limitation is that it only works with human activity recognition scenarios [8].

Yiqiang et al. [9] identified two challenges in smart healthcare. One of them was data islanding, which makes aggregation difficult, and another challenge was personalization. FedHealth was presented to tackle these challenges. FedHealth resolved these two challenges, but its limitation is that it doesn't identify any diseases. It is only useful for detecting human activity [9].

Soumya et al. addressed interoperability, availability, and integration issues. They presented an IoT architecture that strives for smarter, wired, and customized healthcare systems in smart homes. The cornerstone of the planned healthcare scheme was M2M data collection using the M3 architecture. It integrated home automation sensors with wearable data sources to create usable insights and used a lexical reasoning engine to merge possibilities [10].

Juan et al. proposed a telemonitoring framework that increases home security for dependents. It incorporates components for tracking and deployment of alerts, as well as supplementary resources to respond to crises automatically. The authors conducted several test cases to evaluate the system's overall effectiveness, particularly how well it handled crises [11].

Valerie et al. identified a customized health-tracking program using smartphones and wireless (wearable) sensors. Their agenda was to combine ubiquitous computing with mobile health technology. They have identified life-threatening irregular heartbeats remotely on the smartphone, and if the patient is in distress, they will contact the ambulance immediately. The main drawback of the proposed solution is that specificity and sensitivity levels are not defined, and early disease detection through symptoms cannot be detected [12].

Rehman et al. [13] proposed a reputation-aware autonomous FL enhanced by blockchain technology. Since research on blockchain-based reputation structures and FL is still in its early phases, the article provided a wide range of research questions to entice scholars and practitioners to learn more about this fascinating field.

The authors defined the system's workflow in two stages [14]. In the initial stage, the client learns the product's initial model on the mobile edge computing (MEC) server and the cell phone. The second step involves manufacturers selecting clients or organizations to play the role of miners and assessing the observed model using the models acquired from clients. To safeguard customers' privacy and improve test consistency, the authors implemented differential privacy on derived functionality and proposed a new normalization strategy. They invented an incentive mechanism to entice more consumers to develop the FL model. However, their testing did not yield reliable results because it is crucial to identify the ideal parameters for striking a fair balance to attain high test precision. When averaging the locally uploaded model, there should be a balance between the local and global epoch counts.

The authors proposed an IoT-blockchain-based framework for remote healthcare tracking [15]. In the architecture, there are two different kinds of blockchain: (1) Medical equipment (2) Deliberations. Deliberations will be held in addition to the use of blockchain to preserve medical data generated by medical equipment during treatment. Hospitals use blockchain to archive medical information permanently. Smart contracts (Chaincodes in Fabric) are used to check and validate transactions and are performed by supporting peers using the Functional Byzantine Fault Tolerance algorithm. The authors developed a user interface to show patient health information.

A blockchain-based infrastructure was proposed by Dilawar et al. [10] for the secure sharing and storing of significant amounts of sensitive data produced by IoMT. Blockchains can store data without allowing unwanted changes. However, there are still many hurdles to integrating blockchain into industries. The scale of personal healthcare data is much greater than the size of most public blockchains. Storing personal healthcare information (PHRs) on the blockchain is one of the most difficult obstacles. The total complexity of the blockchain will be immense and processing the vast amount of data that needs to be researched further will be incredibly challenging. Blockchain was originally intended to store limited amounts of data in blocks (Bitcoin) [10]. Table 1 compares the current state of the art.

In the previous section, the existing literature highlighted numerous unresolved research questions. In this work, we focus on the problems with data islanding and personalization in wearable medical technology. IoMT architecture employing blockchain technology is required for people in smart homes where wearable sensors allow continuous monitoring of physical parameters.

Table 1. Summary of Related Works.

Paper	Simulator	Experimentation Details	Data Set	Result	Limitation
[7]	Generative convolutional autoencoder (GCAE) boxplot	No. of participants: $K = 5$ Training passes over each client's local data: $E = 5$ Local minibatch size: $B = 10$ Number of local updates per round = $E nk/B$	MobiAct	The precision score of user 1 is 96%, and the average precision score of all 5 users is 90.8%.	It seems that security is not the focus of this work. It offers no solution for the protection of personal data.
[8]	Embedded sensors	Device = Samsung galaxy S3 Sensor = Accelerometer, Gyroscope Activities = 10 Users = 30	MobiAct	Able to achieve superior prediction performance with lightweight models and small communication overhead.	Proposed architecture required cloud computation for personal data. This solution can't work offline.
[9]	Blockchain technology	Accelerometer, Gyroscope are examples of sensors. Users = 30 Activities = 6 Sampling rate = 50 Hz Sensor = Accelerometer, Gyroscope Instance = 10,299 Channel = 9 $N = 0.01$ Batch size = 64 Training epochs = 80	Public human activity recognition dataset called UCI Smartphone	The results of transfer learning significantly outperform no transfer by 4% on average accuracy. This indicates that the transfer learning procedure of FedHealth is highly effective and extensible.	The proposed solution uses KNN, SVM, and random forest (RF) with FedHealth which can make it more complex and put considerable computational cost.

Table 1. Cont.

Paper	Simulator	Experimentation Details	Data Set	Result	Limitation
[16]	M3 Framework Android devices	Mobile application = CCT (Connect & Control things) M2M gateway Sensor & actuator metadata	Real time sensor metadata	The CPU load rises to 15–19% only during the M2M data processing for healthcare and smart home sensors. The application requires less than 3.5 MB memory in Android powered devices. On a Samsung Galaxy S3 running Android KitKat consumes 298 mW and 259 mW when operated on mobile data and Wi-Fi.	Privacy and security of data is lacking in this work.

3. Methodology

3.1. Investigation Objectives

The IoT life cycle is divided into four parts:

- (1) data is gathered using sensors on devices;
- (2) data is kept in the cloud for analysis;
- (3) processed data is returned to the device; and
- (4) the device responds accordingly [17].

We propose a revolutionary IoT device management architecture. The architecture connects a decentralized access control system to regionally dispersed sensor networks. The strategy guarantees that accessibility control laws are obeyed and is based on blockchain technology. This strategy does away with centralized access management by utilizing blockchain technology. If authorization inquiries and changes are made often, a solitary centralized user access server could create a bottleneck.

The client/server architecture was developed to meet the needs of conventional human–machine systems. Internet scenarios where centralized access administration are necessary and endpoints are located in the same trust domain. On the contrary, some IoT cases, wherein IoT systems are transferable and adhere to several control organizations for their lives, are significantly more volatile than typical scenarios.

The Internet of Things (IoT) is the idea that everything will be connected to the Internet. Vehicles, home appliances, and other items with embedded electronics fall into this category, together with the programs, detectors, actuators, and connectors that enable connections, data gathering, and data transmission.

In contrast to existing centralized system approaches [18], our method of IoT access management has the following benefits:

- **Versatility:** The design can be used in various administrative systems or domains. Consequently, each organizational domain can fully administer IoT devices while blockchain regulations still enforce access control norms.
- **Access:** Minimal administrators in certain IoT systems could have sleeping habits that make it difficult to get in touch with them frequently. With this solution, you may always access the access control rules. Additionally, access to data is not restricted if certain administrative servers fail, even though all access control information has been disseminated.
- **Interoperability:** Many managers can access or modify access control settings simultaneously on a restricted device.
- **Convenient:** Our method does not necessitate any changes to IoT devices. Through blockchain networks, the administrators and IoT devices may also connect, enabling cross-platform cooperation.
- **Scalability:** Our method enables a restricted manager to control numerous IoT devices since the IoT devices do not directly get access control information from the managers.

Additionally, our solution allows several IoT devices to connect to a single chain across various constrained networks.

- Critical point: IoT device locations and access points are concealed by the system.

Thus, according to Andres Ricaurte [19], a blockchain's distributed ledger is impenetrable to tampering. As a result, there is less of a requirement for mutual trust between the parties. Due to this, no single party has full control over the enormous volumes of data that IoT devices generate. Since the blockchain is encrypted, no one can modify existing data records. A further layer of protection is added to the network by putting IoT data on the blockchain, prohibiting unwanted attackers from obtaining access. Data protection across the entire IoT ecosystem is a problem for IoT operators. IoT devices are vulnerable to malicious operations, distributed denial-of-service attacks, and data leaks due to security flaws.

For all parties concerned, the marriage of IoT and blockchain opens up new possibilities, decreasing inefficiencies, boosting security, and increasing transparency while enabling secure machine-to-machine transactions. Thanks to the integration of numerous technologies, a physical item may be monitored from the moment it is mined, for example, through every phase of the supply chain until it gets to the final user.

3.2. Integrating Blockchain and IoT

There has been an increase in security. Blockchain technology offers encryption while data is being transported and stored, as well as the capacity to authenticate and approve transactions started by a trusted party. Blockchain technology creates a public ledger of all activities and allows visibility of who has the system's access and who is trading. Additionally, blockchain offers an extra degree of security to the system through encryption, the removal of isolated points of failure, and the capability to instantly identify the network's weak link.

In addition, money can be saved. The entire network could become responsive at a lower cost by streamlining transactional authentication and production conditions on a blockchain.

All transactions are handled promptly. This is particularly true when dealing with supply chains that contain many vendors, manufacturers, dealers, and consumers.

The blockchain's ability to serve as a shared ledger allows for the transmission of raw data between untrusted parties and accelerates transactions by reducing manual procedures.

3.3. Experimental Setup and Data Collection

The data is collected through a source called Fitbit.

Experimental Setups

- Import Python Libraries
- Pandas (For reading and writing Excel and all data frame activities)
- Random (To generate random numbers)
- Twilio.rest (To send SMS)
- Then, our program will read our dummy data set of health data daily.
- Preprocessing: Trimming starting and ending spaces. It will convert the activity day date time.
- Flagging: Flag generation "Warning" or "No Warning" condition based ($\text{avgheartrate} < 60$ or $\text{avgheartrate} > 100$) or ($\text{temperature} < 97$ or $\text{temperature} > 100.4$)
- Then export results in Excel.
- Then Filtering "Warning" 2 records on a sample basis.
- Generate text on condition whether the flag was on absurd heart rate or absurd temperature.
- Adding Phone Number/s on which alerts are sent on the Twilio website.
- Passing Account_SID and Auth-Token in the function "client" of the Twilio library.
- Send a message alert to the number, also added on Twilio.

We presented an empirical analysis to testify to the problems related to blockchain-based federated learning and wearable IoT devices. IoT and blockchain have the possibility of working well together. However, it is vital to remember that IoT and blockchain are not developing at comparable rates. For instance, scalability to handle massive volumes of information, legislative and data protection issues, and standards are all requirements for using blockchain in a business setting. Additionally, IoT technology needs to show that the architecture is reliable, efficient, and secure. It must overcome these challenges until new enterprise solutions become corporate IT norms.

4. Proposed Framework

4.1. Objectives

Here are the objectives for the personalized healthcare architecture. The accessibility and inclusion of a data-generating subsystem from which physical characteristics will be gathered are the first prerequisites of a personalized healthcare architecture. The entire architecture system requires a computing and storage subsystem because data-generating devices cannot do these tasks. Regardless of the network subsystem’s communication mechanisms, the computing and storage subsystems ought to be capable of communicating with the data-generating subsystem. Additionally, a user subsystem that will use the individualized healthcare solutions must be included in the architecture. In order to enable the identification of M2M equipment in the data generation subsystem and the selection of the most appropriate M2M devices for data collection, the consumption component should support resource discovery. Figure 1 shows block diagram of functional IOT architecture for personalized healthcare.

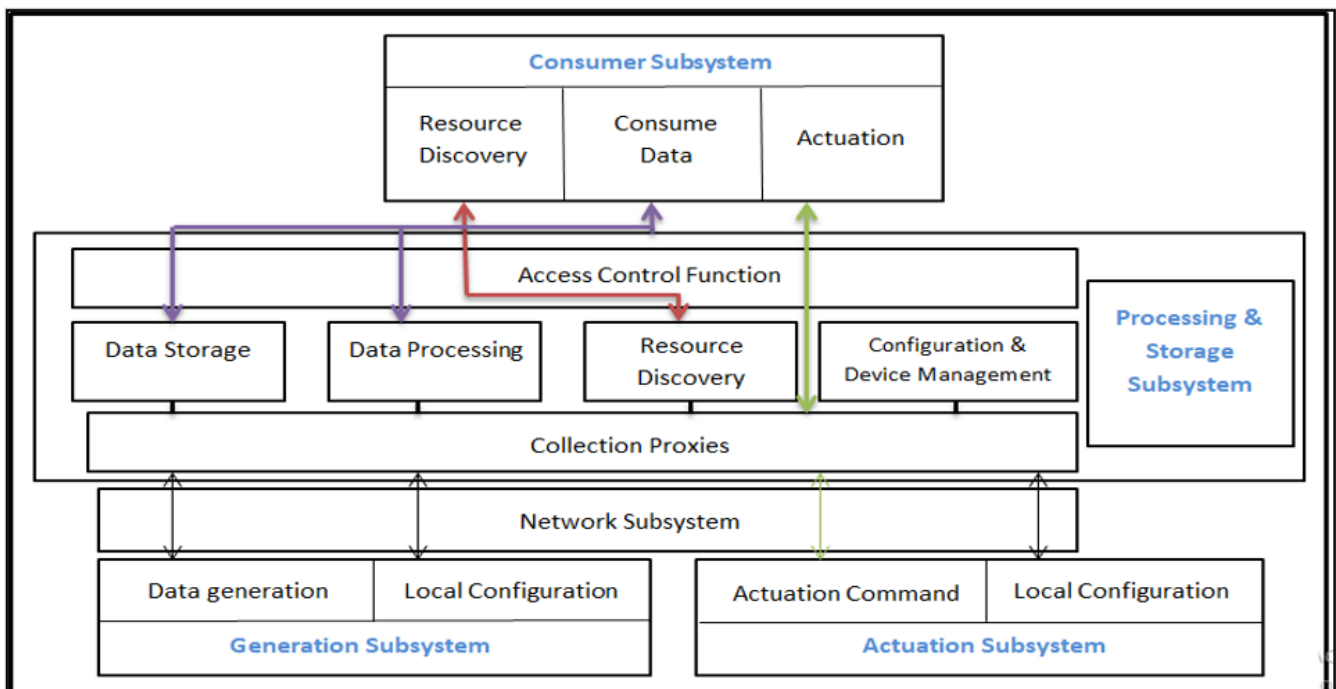


Figure 1. Functional IOT architecture for personalized healthcare.

A remote support framework is necessitated to maintain the enrolled equipment and its modifications. There must be mechanisms in the processing and storing subsystem for increasing production abstraction from original data. This is the initial step toward a healthcare system that is more sophisticated, interconnected, and individualized. The storage and processing subsystem should be capable of sending raw or transformed data, depending on the user’s requirements (high-level abstraction). Using RESTful principles, communication between the aforementioned subsystems should be stateless. To grant au-

thorized users access to advanced healthcare solutions, suitable access control mechanisms must be established. A premium service for a set of events notified via notification should be offered by the complete system.

Since the user receives push notifications, they ought to be able to react to the smart environment. To achieve this, an actuated subsystem must be present. From the perspective of the user, the design must ensure minimal latency, good QoS, an intuitive interface, and integration with social media networks. For AAL-based systems, accessibility, error handling, and prompt feedback are essential.

A blockchain developer must have security skills such as elliptic curve digital signatures, Merkle proofs, cryptographic hashing, private key, public-key cryptography, and many others. Regulatory, legal, and compliance considerations are driving the evolution of security frameworks.

4.2. Blockchain Technology

A blockchain is a digital storage technology that makes it challenging or impossible to alter data or compromise system security. In essence, a blockchain is a shared ledger that contains activities that are replicated and distributed throughout the chain of computer systems that comprise the blockchain. Anyone may verify the chain’s legitimacy thanks to the blockchain’s shared functionality. Each block in the thread is a digital record or interaction that is timestamped and associated with a specific participant. When a block is formed, it is given a unique hash that reflects both its identity and its contents. Not only does moving everything within a block cause a complete shift in the local hash, it also causes a complete shift in all subsequent blocks. Figure 2 provides block diagram of an example blockchain network.

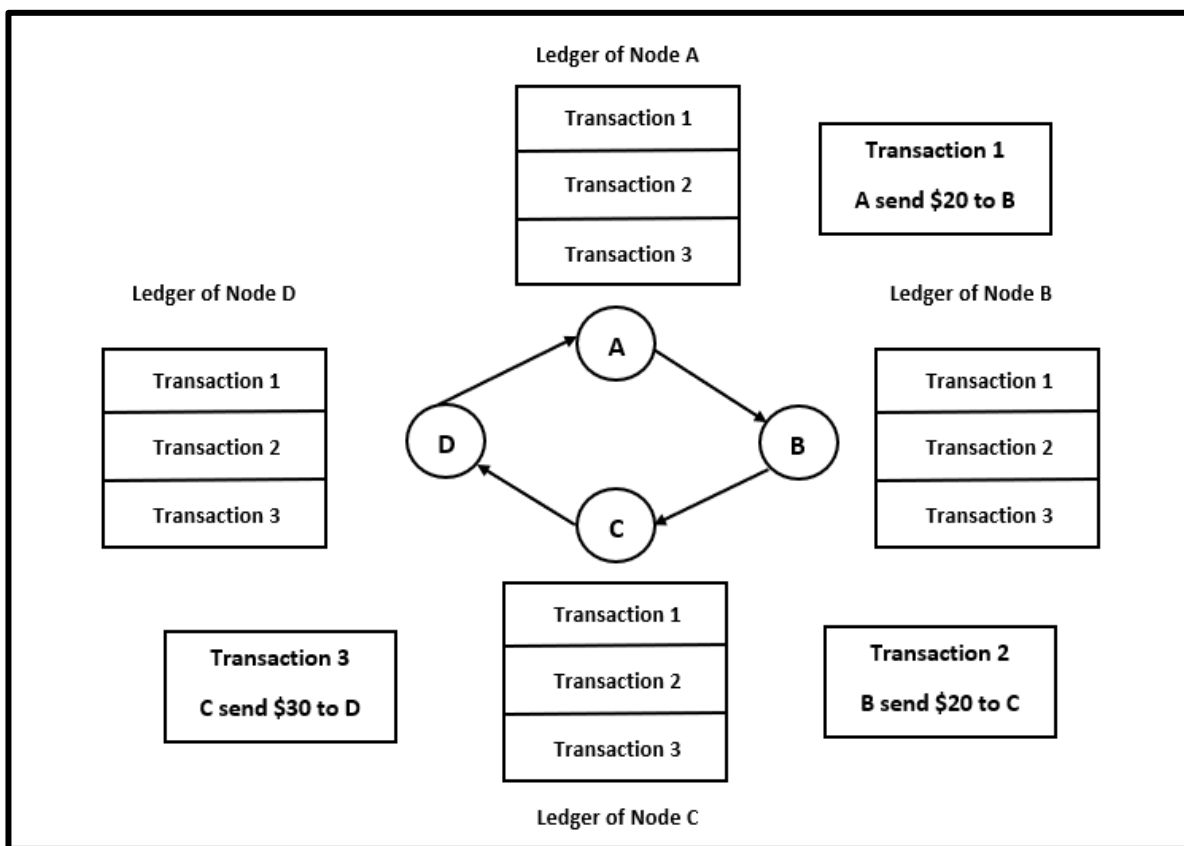


Figure 2. Blockchain Technology Example.

4.3. Blockchain Network

Ethereum was the blockchain technology considered for the proof of concept. We provided a prototype on the exclusive Ethereum network behind a bogus genesis block. Since the prototype's features are more detailed than those of a public blockchain, we tried to review the system using a private blockchain. The idea is to use it in practical situations on open blockchains.

Ethereum, a platform that can code, uses Resilience, a Turing-complete programming language, to develop, distribute, and carry out smart contracts. These contracts are stored on the blockchain and can be as large as desired.

In Ethereum, there are two different types of accounts. Private keys maintain the externally held accounts, whereas contract code manages the contract accounts. When a message is received by the contract account, the code is carried out. The agreement is executed under a contract account, and all of the administrators in our design are externally owned accounts.

4.4. Blockchain Meets IoT

The Internet of Things (IoT), a key component of the next-generation Internet, is expanding and consolidating its position. One of the technical issues is the ability to handle the billions of devices that are distributed throughout the globe. Although there are user access solutions for the Internet of Things, their centralized architecture creates new technological challenges when trying to regulate them internationally.

4.4.1. IoT Decentralized Access Control System Overview

The architecture described in this study establishes a ground-breaking decentralized control access system that disseminates and stores access control data using blockchain technology. Despite the IoT and organizational hub nodes, all entities will employ blockchain technology. Every node in a blockchain network needs to have a copy of the blockchain. The chain has potential and has already begun to expand dramatically. Most IoT systems will not be capable of storing blockchain data due to their constraints. As a result, our architecture replaces the exclusion of IoT devices from the blockchain with an administration hub. This separate component requests permission data from the blockchain on behalf of IoT devices.

Moreover, the solution includes a single shared ledger that lists every action the access control system takes. It is a unique contract that cannot be removed from the database. Administrators communicate with contracts to configure the system's access control policy.

4.4.2. System Architecture

Six different components make up the architecture:

- Wireless Sensor Networks
- Managers
- Agent Nodes
- Smart Contracts
- Blockchain Networks
- Management Hubs

Wireless Sensor Networks: A sort of communication system called a wireless sensor network enables irregular connectivity in low-light and low-power environments. IoT devices in the wire-free sensor network also have limited processor, memory, and energy availability. IoT devices are not part of the blockchain network. Since all parts of the public blockchain must be completely traceable, this is one of our architectural goals. The challenge of producing large, unique random numbers may be solved using public key generators. Existing IoT encryption technology would typically produce a public key for each device. As a result, establishing encrypted connections will preserve unique IDs. CoAP, one of the most widely used IoT communication protocols, already supports DTLS for secure connections.

Managers: The person or entity in charge of the access control rights for a collection of IoT devices is known as a “manager”. Managers are frequently referred to as “lightweight” nodes in our system. Unlike mining nodes, lightweight nodes do not keep blockchain data or verify blockchain transactions. Therefore, restricted devices can act as administrators in our network without being constrained by their hardware. Additionally, managers who utilize our system can save money on hardware because they do not need to be constantly linked to the blockchain network. A manager could be anyone or anything. IoT systems, in contrast, require manager oversight to be registered. This prevents administrators from enrolling controlled devices without the devices’ consent. At a minimum, one authorized management entity must own each registered IoT device. Otherwise, nobody could operate the machinery. Several managers might simultaneously own a connected IoT device. Managers can create particular access control privileges for IoT devices once they have been placed under their supervision.

Agent Node: In our architecture, the agent node is a specialized network server in charge of distributing the sole smart contract for our system. The agent node is the smart contract owner for the duration of the access control system. When the smart contract is accepted into the network, the agent node acquires an identifier that sets it apart from the blockchain network once more. The smart contract address must be known to all nodes in the blockchain network for them to communicate with it.

Smart Contract: The activities specified in a single smart contract serve as the rules for the access control system described in this study. This unique smart contract will never be deleted from the network. As a result, the access management system’s processes activated by blockchain transactions are all specified in the smart contract. The miners will keep the transaction’s details globally available once it has started an operation. The smart contract and its actions can be accessed from any location on the planet. Additionally, managers are the only entities that may engage with the smart contract to change the system’s policies, which also needs to be considered.

Private Blockchain Network: For simplicity, the blockchain network in the architecture is a private blockchain. We used a private blockchain to analyze the system because the prototype’s components have more dimensions. Remote nodes can only write to private blockchains; others can only read from them. Miners in the network contribute to network security and stability by approving transactions and keeping copies of the blockchain. Nodes can track and retrieve global access policies for specific devices via the blockchain interface. The data is decentralized and unaffected by manipulation.

Management Hubs: As mentioned previously, IoT devices are not included in the blockchain network. Most IoT devices have severe CPU, storage, and battery capacity limitations. These restrictions make it challenging for IoT devices to connect to the blockchain network. Being a part of the blockchain network entails preserving a localized copy of the blockchain and taking note of network transactions.

As a result, we have decided to use the control hub node. IoT device CoAP messages are transformed into JSON-RPC commands that blockchain networks can understand through a user interface known as the management hub. A blockchain node, such as a miner, is directly connected to the administrative center. Numerous management hub nodes can connect to the same blockchain node, and a single management hub node can interact with multiple sensor networks. IoT devices will only access the management center to query the blockchain for data.

The management hub’s nodes are not permitted to be restricted objects. IoT devices must have great performance features to handle as many simultaneous queries as possible.

In the simplest case, any IoT gadget can link to any control hub and contact the blockchain network without requiring authentication. However, there are many circumstances where access restrictions are required. In this case, there will be a limited number of management hubs to which IoT devices can connect. Each IoT device that is added to the system requires a manager node which must communicate the device’s location and

credentials to the chosen management hub node. Figure 3 illustrates blockchain enabled IoT architecture.

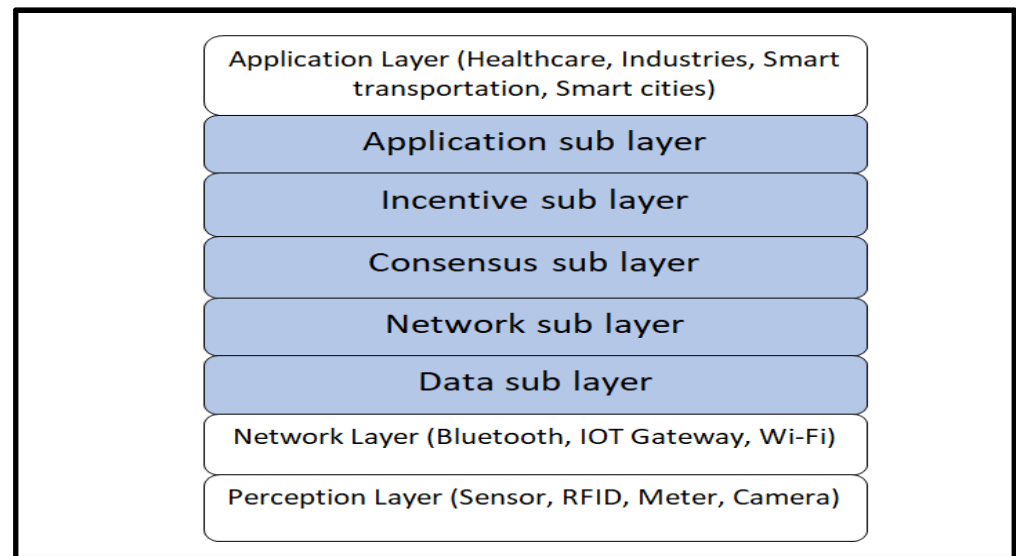


Figure 3. Blockchain-enabled IoT architecture.

4.5. Federated Learning

Federated learning (FL), a new breed of machine learning, is the most promising approach for delivering learning to end devices without releasing private information to a central server. In the FL mechanism, end devices and the central orchestrator only exchange parametric updates, and the central server serves as an orchestrator to initiate the FL learning process. Although FL is still in its early stages of development, many organizations have not yet accepted it. Owing to unidentified privacy issues, it can improve privacy and data management. Issues with device heterogeneity and personalization have been solved using the FL algorithm. The FL technique involves sharing model parameters with the central server to update the global model after using end-device data to train the local model. The modified global model parameters are then used to train the local model.

Only the parameters of the model are shared through FL, safeguarding the privacy of the data. However, concerns about privacy and the best use and distribution of resources still exist. Due to their resource limitations, end devices might not be capable of sharing model parameters with the central server. In this situation, a collaborative FL approach was developed to help eliminate devices [18]. The database controller in collaborative FL receives model parameters from end devices that are prompted to share them with neighboring devices, which subsequently composite the local model data.

FL is utilized in settings where confidential data is handled owing to its privacy-preserving features. While exchanging parameters of the model and consuming excessive communication networks expose the FL process to additional dangers, such as an attacker changing parameter estimation to get access to sensitive data, FL partially addresses the privacy difficulties related to centralized ML techniques [20]. We need a thorough assessment of any potential privacy issues in the FL process to ensure that we correctly utilize the process's properties for the application.

Heterogeneity through Clustering

The gadgets in the IoT system gather a variety of data. The global model consolidation algorithm based on FedProx [21], which incorporates weight parameters in the FedAvg algorithm, was developed for this purpose. Appropriate weight selection is a difficult and time-consuming procedure. Furthermore, using the FedProx algorithm does not guarantee that the FL method's performance will improve any further. As a result, dealing with such

a case scenario necessitates the use of a heterogeneous algorithm. The data collected by devices in the Internet of Things system network is diverse. For this, the FedProx-based global model aggregation method [21] was created, which incorporates weight factors in the FedAvg. Incorporating the correct weight is a challenging and time-consuming process. Using the FedProx algorithm also does not guarantee that the FL method's performance will increase any further. As a result, dealing with such a scenario necessitates the use of a heterogeneity-aware algorithm [22].

4.6. Federated Learning and Blockchain Integration

We examined a trustworthy blockchain-based federated learning architecture to dramatically improve the openness and fairness of federated learning systems. Due to its immutability, blockchain has been used in federated learning and the Internet of Things to ensure data integrity. To begin, blockchain's transparency attribute assures that all documents written on the blockchain are auditable by all allowed parties. Furthermore, the immutability of blockchain and smart contracts promotes accountability by preventing anyone from changing records once they have been published on the blockchain.

Due to the disadvantages of using a centralized system for data storage and management, researchers are focusing on adopting a decentralized strategy to store and manage data acquired from IoT devices [23]. Due to its public ledger, customizability, privacy, and provenance features, which enable secure data storage without involving other organizations, blockchain was brought into the picture for IoT technology.

Our blockchain-based, trustworthy FL architecture design calls for installing at least one blockchain node on each client and the main server. They are able to establish a network as a result. The entire transaction data is kept locally by each node as a chain of blocks. All subsequent blocks recorded at all involved nodes must reflect any changes to earlier data states. Additionally, smart contracts, in which each participant is recognized by their specific blockchain address, are typically used in blockchain activities for data-model provenance. These features of blockchain can help federated learning become more accountable. All model parameters (local and global models) are stored in off-chain databases of local models and databases of global models during each federation epoch. To enable data and model provenance and co-versioning in the interim, hashed local data versions are created and stored in the on-chain data-model registry smart contract. The data is hashed, and the date and information volume are added to the hashed data before it is broadcasted to the blockchain.

On client devices and the main server, database systems are used to store the actual local and global models. On the chain, only the hashed versions of the models are kept. Despite our best efforts, the model size is too large for the ongoing federated learning processes, even though we sought to store both local and global models completely on blockchain (upload, aggregation, and download operations). We can guarantee that the record of both models is unalterable and transparent to the relevant stakeholders by storing only the hashed versions of them on a chain. By comparing an off-chain model's hash value to the matching on-chain record, one can verify a model's origin. This allowed the architecture to execute model provenance utilizing the off-chain data storage design pattern while maintaining the viability and efficacy of the federated learning process [24]. Models were simply hashed and stored on the blockchain, while the original model was preserved in database systems.

5. Results & Discussion

IoT technology is employed in many industries today, including healthcare, agriculture, and smart cities. IoT is applied in healthcare for ongoing patient health monitoring, medicine tracking, and more. However, by fusing IoT and blockchain, a number of security issues with IoT can be resolved. A decentralized technology that can be used to increase system security is the blockchain.

Blockchain technology guarantees that patients’ private health records are shielded from tampering and leaks in the healthcare industry.

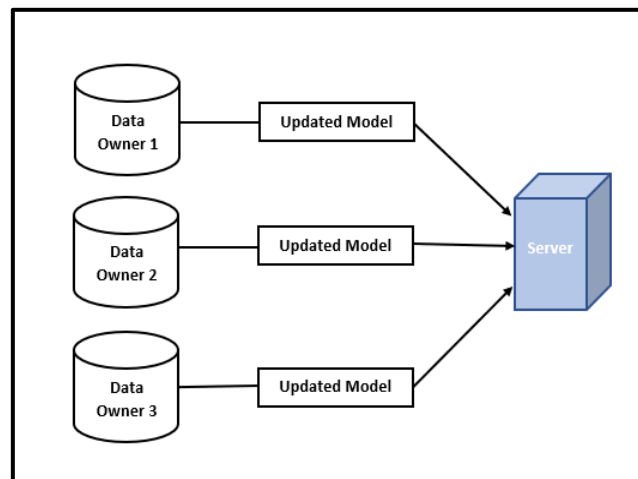
In order to boost actual quality and enhance the current healthcare sector, this study made an effort to list all the potential integrations of blockchain and IoT technologies into the healthcare industry. The application of IoT and blockchain technologies to managing medical records and remote patient monitoring, respectively, was thoroughly examined. The implementation of these two technological breakthroughs, namely IoT and blockchain, in the healthcare sector was also studied and discussed, along with several potential challenges and concerns. According to the study’s conclusions, it is clear that these two methods hold great promise for the healthcare business and that their integration will transform the sector as a whole.

5.1. Patients Health Record

This section presents the graphical representations of the data collected using IoT gadgets.

5.1.1. Calories Burned Based on Daily Steps

Figure 4b depicts how many calories are burned per day based on the number of steps taken. In Figure 4c, its graphical representation is given.

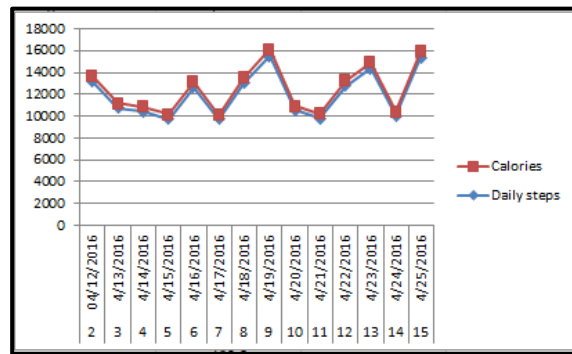


(a)

ID	Activity Day	Daily steps	Calories
2	04/12/2016	13162	526.48
3	4/13/2016	10735	429.4
4	4/14/2016	10460	418.4
5	4/15/2016	9762	390.48
6	4/16/2016	12669	506.76
7	4/17/2016	9705	388.2
8	4/18/2016	13019	520.76
9	4/19/2016	15506	620.24
10	4/20/2016	10544	421.76
11	4/21/2016	9819	392.76
12	4/22/2016	12764	510.56
13	4/23/2016	14371	574.84
14	4/24/2016	10039	401.56
15	4/25/2016	15355	614.2

(b)

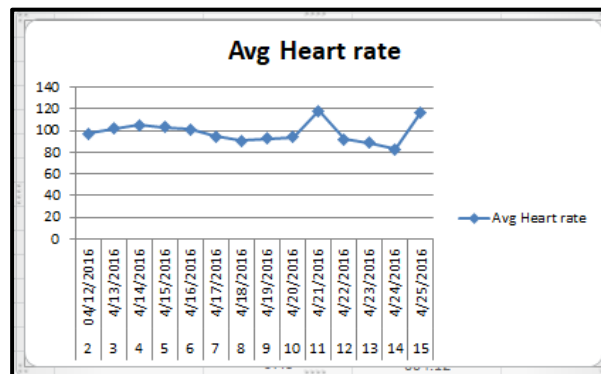
Figure 4. Cont.



(c)

ID	Activity Day	Avg Heart rate
2	04/12/2016	97
3	04/13/2016	102
4	04/14/2016	105
5	04/15/2016	103
6	04/16/2016	101
7	04/17/2016	95
8	04/18/2016	91
9	04/19/2016	93
10	04/20/2016	94
11	04/21/2016	118
12	04/22/2016	92
13	04/23/2016	89
14	04/24/2016	83
15	04/25/2016	117

(d)

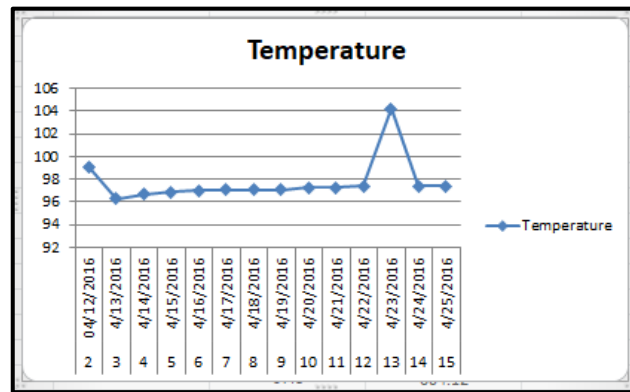


(e)

ID	Activity Day	Temperature
2	04/12/2016	99.1
3	04/13/2016	96.3
4	04/14/2016	96.7
5	04/15/2016	96.9
6	04/16/2016	97
7	04/17/2016	97.1
8	04/18/2016	97.1
9	04/19/2016	97.1
10	04/20/2016	97.3
11	04/21/2016	97.3
12	04/22/2016	97.4
13	04/23/2016	104.2
14	04/24/2016	97.4
15	04/25/2016	97.4

(f)

Figure 4. Cont.



(g)

Figure 4. (a) Federated Learning Architecture. (b) Dataset including daily steps and calories. (c) Graphical representation of calories based on daily steps. (d) Average Heart Rate Dataset. (e) Graphical representation of heart rate. (f) Dataset of Body Temperature Per Day (g) Graphical representation of body temperature.

For example, on 4 December 2016, almost 526 calories were burned after taking 13,162 steps. In general, most people burn about 0.04 calories per step. It seems like a minuscule amount, but getting 13,162 steps per day can add up to an extra 526.48 calories, or, in terms of food, about an extra cheeseburger.

The formula is:

$$\text{No. of daily steps} * 0.04 = \text{calories}$$

5.1.2. Average Heart Rate

In Figure 4d, the average daily heart rate of a person is measured through sensors.

In Figure 4e, its graphical representation is given. Individuals over 10 years of age, including older adults, should have a resting heart rate between 60 and 100 beats per minute (bpm). A warning will be generated if the heart rate is less than 60 or more than 100. A warning SMS will be sent to the health provider.

5.1.3. Body Temperature per Day

Figure 4f depicts how a person’s temperature is measured every day using sensors.

In Figure 4g, its graphical representation is given. The average body temperature is 98.6 °F (37 °C). A warning will be generated if the temperature is less than 97 or more than 100.4 °F. A warning SMS will be sent to the health provider (Figure 4f).

5.2. Warning and Alarm Generation

Wearable gadgets, like smartphones and wristbands, make it simple to obtain information about people’s health, including activities, sleep, sports, etc., thanks to the rapid development of computing technology. We adopted some data from Fitbit. We first took 500 values with average heart rate and average body temperature as parameters and analyzed the data with a Python code to determine if there were any warnings. Individuals over 10 years of age, including older adults, should have a resting heart rate of between 60 and 100 beats per minute (bpm). If the heart rate is less than or equal to 100, a warning will be generated. The average body temperature is 98.8 degrees Fahrenheit (37 degrees Celsius). A warning will be generated if the temperature is less than 97 or more than 100.4. A warning SMS will be sent to the health provider.

If (avgheartrate < 60 or avgheartrate > 100) or (temperature < 97 or temperature > 100.4)

Warning

Else

No Warning

5.3. Warning and Alarm SMS Generation

5.3.1. Twilio

The Twilio API is also called an SMS API. Twilio's Programmable SMS API allows you to integrate powerful messaging capabilities into your apps. Using this REST API, one can send and receive SMS messages, monitor the transportation of sent texts, and access and modify message histories. The SMS API from Twilio is a versatile building element that can let you go from sending your first text message to sending and receiving millions.

5.3.2. How to Make an Account on Twilio

Creating an account on Twilio is quite simple.

1. Go to Twilio's new account page and sign up for an account and provide the:
 - ✓ First Name
 - ✓ Last Name
 - ✓ Email Address
 - ✓ A password that meets Twilio's requirements
2. Verify your email address:
 - ✓ Twilio will send an email to the address that the account was registered with.
 - ✓ Click or copy the link and login to the account
 - ✓ Upon successful login, your email should be verified
3. Verify a phone number.
 - ✓ Twilio needs to verify that the user is a real person/organization. The phone number used will only be used for verification.

To verify:

- ✓ Select your country and enter a phone number.
 - ✓ Enter the verification code received.
4. Get started by following the prompts To get to your dashboard:
 - ✓ Select "No" when asked if one writes code.
 - ✓ Select "Skip to dashboard" when asked the purpose of using the program.
- After this, the account is set up, and you'll have made it to the dashboard. To set up billing:
- From the dashboard, click Billing from the menu.
 - Select "Upgrade Now"
 - Enter the company's legal address
 - Enter the billing address associated with the credit card that will be used for billing.
 - Hit the "Upgrade Account" button at the bottom of the screen.

5.3.3. Warning SMS Generation

Then, to generate a warning SMS, we signed up on Twilio, imported the client from Twilio Rest, and put it in the Python code. Twilio will now send an SMS to a number we have signed up for whenever there is an abrupt heart rate or an increase or decrease in body temperature.

For example, in Figure 5, we have received two warning messages. The conditions were already set in the code.

Condition is:

If (avgheartrate < 60 or avgheartrate > 100) or (temperature < 97 or temperature > 100.4)

Warning

Else

No Warning

Message one was received when the heart rate dropped below 60. Individuals over the age of 10, including older adults, should have a resting heart rate of between 60 and 100 beats per minute (bpm).

Message two was received when the body temperature increased above 100.4. The average body temperature is 98.6 °F (37 °C). A warning will be generated if the temperature is less than 97 or more than 100.4

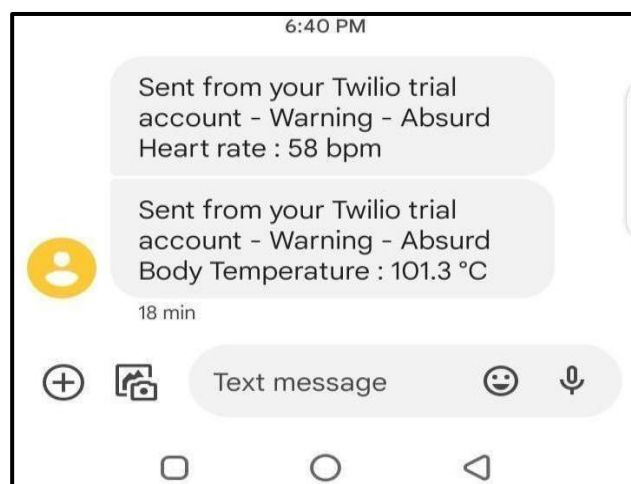


Figure 5. Alert Generate SMS.

5.4. Challenges

The limits imposed by the limited battery life of various IoT devices are one of the main obstacles to the integration of blockchain with IoT.

There are few limitations because certain IoT gadgets are constantly connected to power and Wi-Fi. Many IoT gadgets, however, are not. Additionally, running a blockchain transaction network on a small device is impossible due to its high processing and bandwidth requirements. As a result, they may need to rely on server-based infrastructure or seek assistance from a gateway device or other comparable device. As a result, these ecosystems will have to be rather cooperative by nature.

Furthermore, the security of a gadget is only as good as the infrastructure's weakest link.

Thus, if we have a highly sophisticated hack-resistant blockchain network, but the OS system that my device runs on isn't patched, maintained, or updated, the device may be rendered useless, and the device can easily be hacked at the edge [19].

6. Open Issues

In [25–27], authors have presented blockchain based federated learning solutions for the IoT and tried to solve the problems. The problem of privacy and leakage of information still remains an open issue; Man-in-the-middle attacks are also an open issue. Even though the federated learning-based models claim to protect the privacy of data, due to the distributed nature of those models, they are vulnerable to attacks from some malicious users. Reliability is another challenge; the data and the communication between the devices also require a reliable communication mechanism. As sensors and actuators are used in IoT devices, it is essential to use them efficiently so that the battery consumption remains within the desired limit.

7. Conclusions

The integration of IoT devices and applications has dramatically benefited the modern world. On the other side, technological advancements have brought along many new challenges, including managing data and maintaining confidentiality. In light of these situations, we describe a blockchain-enabled IoT system and its application that employ

privacy preservation mechanisms to improve their privacy. Managing remote data while protecting privacy, on the other hand, remains a difficult task. The FL algorithm, which encourages on-device machine learning through decentralized learning, is specifically designed for this purpose.

Finally, our method's utilization of blockchain technology was built expressly to handle scalability and offer superior results in lightweight IoT applications. This study examines the scalability challenge of controlling access to the IoT's billions of limited devices. even if it is just carried it out on a small scale. Centralized access control solutions are unable to handle growing traffic efficiently. The research presents a new access management system for many limited IoT devices. The blockchain technology-based system is entirely decentralized, since the majority of Internet of Things (IoT) devices can only directly support blockchain technology.

Author Contributions: Conceptualization, K.F. and H.J.S.; methodology, K.F.; investigation, A.O.I.; resources, A.G.; writing—original draft preparation, K.F.; writing—review and editing, H.J.S., S.O.A. and W.N.; visualization, A.O.I.; supervision, H.J.S.; project administration, A.G., S.O.A. and W.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The abbreviations used in this paper are given as follows:

IoT	Internet of Things
IoMT	Internet of Medical Things
WHO	World Health Organization
FL	Federated Learning
MEC	Mobile Edge Computing
PHR	Personal Healthcare Information
SMS	Short Message Service
CoAP	Constrained Application Protocol
DTLS	Datagram Transport Layer Security
ML	Machine Learning
FedAvg	Federated Averaging
bpm	Beats Per minute
API	Application Programming Interface

References

1. Rehman, A.; Razzak, I.; Xu, G. Federated Learning for Privacy Preservation of Healthcare Data from Smartphone-based Side-Channel Attacks. *IEEE J. Biomed. Health Inform.* **2022**, *1*. [[CrossRef](#)] [[PubMed](#)]
2. Rocha Filho, G.P.; Brandão, A.H.; Nobre, R.A.; Meneguette, R.I.; Freitas, H.; Gonçalves, V.P. HOsT: Towards a Low-Cost Fog Solution via Smart Objects to Deal with the Heterogeneity of Data in a Residential Environment. *Sensors* **2022**, *22*, 6257. [[CrossRef](#)] [[PubMed](#)]
3. Gonçalves, V.P.; Mano, L.Y.; Bonacin, R. FlexPersonas: Flexible design of IoT-based home healthcare systems targeted at the older adults. *AI Soc.* **2021**, *36*, 955–973. [[CrossRef](#)]
4. Rocha Filho, G.P.; Meneguette, R.I.; Maia, G.; Pessin, G.; Gonçalves, V.P.; Weigang, L.; Ueyama, J.; Villas, L.A. A fog-enabled smart home solution for decision-making using smart objects. *Future Gener. Comput. Syst.* **2020**, *103*, 18–27. [[CrossRef](#)]
5. Filho, G.P.R.; Ueyama, J.; Villas, L.A.; Pinto, A.R.; Gonçalves, V.P.; Pessin, G.; Pazzi, R.W.; Braun, T. Nodepm: A remote monitoring alert system for energy consumption using probabilistic techniques. *Sensors* **2014**, *14*, 848–867. [[CrossRef](#)] [[PubMed](#)]
6. Filho, P.G.; Villas, L.A.; Gonçalves, V.P.; Pessin, G.; Loureiro, A.A.; Ueyama, J. Energy-efficient smart home systems: Infrastructure and decision-making process. *Internet Things* **2019**, *5*, 153–167. [[CrossRef](#)]
7. Wu, Q.; Chen, X. FedHome: Cloud-Edge Based Personalized Federated Learning for In-Home Health Monitoring. *IEEE Trans. Mob. Comput.* **2020**, *21*, 2818–2832. [[CrossRef](#)]
8. Wu, Q.; He, K.; Chen, X. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. *IEEE Open J. Comput. Soc.* **2020**, *1*, 35–44. [[CrossRef](#)] [[PubMed](#)]

9. Chen, Y.; Wang, J.; Yu, C.; Gao, W.; Qin, X. FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare, Beijing Key Lab. In *Mobile Computing and Pervasive Devices, Institute of Computing Technology; CAS 2University of Chinese Academy of Sciences: Beijing, China, 2020*.
10. Dilawar, N.; Rizwan, M.; Ahmad, F.; Akram, S. Blockchain: Securing internet of medical things (IoMT). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [[CrossRef](#)]
11. Corchado, J.M.; Bajo, J.; Tapia, D.I.; Abraham, A. Using Heterogeneous Wireless Sensor Networks in a Telemonitoring System for Healthcare. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *14*, 234–240. [[CrossRef](#)] [[PubMed](#)]
12. Gay, V.; Leijdekkers, P. A health monitoring system using smart phones and wearable sensors. *Int. J. ARM* **2007**, *8*, 29–35.
13. Rehman, H.U.; Mohammad. Towards Blockchain-Based Reputation—Aware Federated Learning. In Proceedings of the IEEE Conference on Computer Communications Workshops, Toronto, ON, Canada, 6–9 July 2020.
14. Zhao, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2019**, *8*, 1817–1829. [[CrossRef](#)]
15. Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C. An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–5.
16. Datta, S.K.; Bonnet, C.; Gyrard, A.; Da Costa, R.; Boudaoud, K. Applying Internet of Things for personalized healthcare in smart homes. In Proceedings of the 2015 24th Wireless and Optical Communication Conference (WOCC), Taipei, Taiwan, 23–24 October 2015; pp. 164–169.
17. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *Hindawi J. Food Qual.* **2021**, *2021*, 7608296. [[CrossRef](#)]
18. Li, C.; Zhang, L.J. A blockchain based new secure multi-layer network model for internet of things. In Proceedings of the 2017 IEEE International Congress on Internet of Things (ICIOT), Honolulu, HI, USA, 25–30 June 2017; pp. 33–41.
19. Lauren Horwitz and Second Linda Rosencrance, “How Blockchain Technology Can Benefit the Internet of Things”, 31 May 2021. Available online: <https://www.iiotworldtoday.com/2021/05/31/how-blockchain-technology-can-benefit-the-internet-of-things/> (accessed on 1 December 2022).
20. Narayanan, A.; Shmatikov, V. Robust deanonymization of large sparse datasets. In Proceedings of the IEEE symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 111–125.
21. Li, T.; Sahu, A.; Zaheer, M.; Sanjabi, M.; Talwalkar, A.; Smith, V. Federated optimization in heterogeneous networks. *Proc. Mach. Learn. Syst.* **2020**, *2*, 429–450.
22. 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](#)]
23. Novo, O. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [[CrossRef](#)]
24. Xu, X.; Pautasso, C.; Zhu, L.; Lu, Q.; Weber, I. A pattern collection for blockchain-based applications. In Proceedings of the 23rd European Conference on Pattern Languages of Programs. EuroPLoP ’18, New York, NY, USA, 4–8 July 2018.
25. 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](#)]
26. Chang, Y.; Fang, C.; Sun, W. A blockchain-based federated learning method for smart healthcare. *Comput. Intell. Neurosci.* **2021**, *2021*, 4376418. [[CrossRef](#)] [[PubMed](#)]
27. Campanile, L.; Marrone, S.; Marulli, F.; Verde, L. Challenges and Trends in Federated Learning for Well-being and Healthcare. *Procedia Comput. Sci.* **2022**, *207*, 1144–1153. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.