Measurement: Sensors 33 (2024) 101176

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

A blockchain based federated deep learning model for secured data transmission in healthcare Iot networks

G. Ganapathy [a,*], Sujatha Jamuna Anand [b], M. Jayaprakash [c], S. Lakshmi [d], V. Banu Priya [e], Samuthira Pandi V [f]

[a] Department of Mathematics, R.M.D Engineering College, India
[b] Department of ECE, Loyola Institute of Technology, India
[c] Department of IT, R.M.K. Engineering College, India
[d] Department of EEE, Panimalar Engineering College, India
[e] Department of Mathematics, R.M.K. College of Engineering and Technology, India
[f] Centre for Advanced Wireless Integrated Technology, Chennai Institute of Technology, Chennai, Tamil Nadu, India

ARTICLE INFO

Keywords:
Security
Healthcare IoT
Blockchain
Federated learning

ABSTRACT

The wide use of sensors in healthcare applications has made it necessary to have secure communication in healthcare Internet of Things (IoT) networks. The sensor data is sensitive, and can contain extremely confidential information such as medical diagnosis, clinical records, vital signs and health data of patients. The emergence of blockchain as a technology ensures consensus and trust among systems, and is now considered to be a new trend used to achieve high scalability, data integrity and privacy. Federated learning is a new technology based on distributed learning that exploits the concept of trust. In federated learning, each user builds an individual distributed model to help a central server that is accessible only to a trusted user group. This paper harnesses the potential of these approaches and proposes an attack detection model to discern normal user behaviours from that of adversaries in an IoT network. This model is called the Blockchain enabled Federated Learning model for secured communication in healthcare IoT (BFL-hIoT), to secure data in healthcare IoT networks. This model is trained and tested on a standard dataset and demonstrates the highest classification accuracy of 97.16 % for normal, 0.9546 for backdoors, 0.9618 for XSS etc., outperforming other blockchain and deep learning models.

1. Introduction

The combination of Internet of Things (IoT) technology with the healthcare industry is referred to as "healthcare IoT.' This combination has been identified as a key facilitator for improving patient outcomes and reducing the cost of healthcare [1]. The use of smart devices, sensors, and wearable gadgets in the medical field as part of the IoT technology enables the collecting and transfer of data on the well-being and health of patients. The evaluation of this data is done with the goals of improving patient care, preventing sickness, and monitoring existing health issues. Telemedicine services, which allow patients to contact with healthcare practitioners remotely [2] may also be included in this category if appropriate.

Despite this, the expanding usage of IoT in healthcare raises concerns over the confidentiality and safety of critical patient data. Due of this, the effective adoption of healthcare IoT needs secure data transfer and storage that protects patients' privacy [3]. Privacy restrictions in the healthcare business, which includes medical histories, diagnoses, and treatments [4]. Because of these requirements, PHI will always be kept in the strictest confidence. Because unauthorized access to this information could lead to identity theft, financial fraud, and other destructive behaviors [5,6], the gathering and storage of such data by healthcare IoT devices raises significant privacy concerns. These issues are raised as a result of the fact that these devices collect and store such data.

Blockchains are used in cryptocurrencies like bitcoin and ethereum [7]. A block may only be added to the blockchain if it is already in existence. The transactions carried out in each block are connected to those carried out in the block that came before it on the chain. Because of this, the data that is captured will keep both its integrity and its security even after it has been saved.

* Corresponding author.
E-mail addresses: barathganagandhi@gmail.com (G. Ganapathy), sujja13@gmail.com (S.J. Anand), mjh.it@rmkec.ac.in (M. Jayaprakash), elzie.moses@gmail.com (S. Lakshmi), spriya.maths@gmail.com (V.B. Priya), samuthirapandiv@citchennai.net (S. Pandi V).

https://doi.org/10.1016/j.measen.2024.101176
Received 3 April 2023; Received in revised form 6 January 2024; Accepted 30 April 2024
Available online 6 May 2024

It is an ideal tool for healthcare providers to use in their efforts to earn patients' confidence and enhance data privacy by limiting access to sensitive patient health information (PHI) to only those who have been granted permission to see it [8]. Blockchain's inherent security and transparency make it an ideal tool for healthcare providers to use in their efforts to use. One example of a potential use of blockchain technology in the Internet of Things that might arise in the healthcare sector is the implementation of Electronic Medical Record (EMR) systems that are based on blockchain technology. These systems could be able to provide a platform for the storing and delivery of patient health information that is both secure and centralized at the same time. This makes it possible for medical professionals to gather the information they want in order to deliver therapy that is successful [9]. This will assist in the delivery of medical care that is coordinated across the entirety of the healthcare ecosystem [10].

Deep learning is a method of artificial intelligence (AI) that involves the use of multiple data layers to extract features through the processing of multiple data forms using mathematical models such as mathematical algorithms, heuristics, and non-linear methods. This is done for the purposes of analysis and decision-making [11]. In IoT sector of healthcare, deep learning has been put to use to develop a data repository of patient states, to identify potential healthcare difficulties, and to enhance patient therapy. The healthcare industry makes use of deep learning in order to improve health monitoring by allowing for remote monitoring of patient condition (for example, fall detection and sleep tracking), monitor patient-treatment outcomes (for example, glucose monitoring and heart rate monitoring), and predict the risk of healthcare-related complications (for example, falls) [12]. It has recently come to light that the use of deep learning in the medical field may facilitate the growth of DSS as well as EHR. This serves to enhance the overall quality of healthcare choices and minimizes the likelihood of patients receiving substandard treatment [13].

The medical sector's convergence of blockchain technology and deep learning The Internet of Things is able to maximize both the data privacy and the data security of existing technologies while also improving overall productivity. Because of this, it is able to provide a safe environment in which to keep the information pertaining to patients and provide care management services that are both effective and efficient. Deep learning algorithms could be used to analyze and gain insights from this data, while blockchain technology might provide a secure and decentralized platform for storing and processing sensitive patient data. Deep learning algorithms could be used to assess and get insights from this data. The distributed ledger technology (Blockchain) is another option for storing and processing this data. It is likely that this link will make it feasible for healthcare professionals and stakeholders to exchange data in a manner that is both secure and transparent. This would give support to the construction of collaborative care models, which may result in better patient outcomes.

The BDSDT that was developed by Kumar et al. [14] has been built specifically for the purpose of ensuring the safety of data transmission in healthcare IoT systems. This was the primary motivation behind the construction of this method. This approach takes use of a scalable blockchain architecture that integrates a Zero Knowledge Proof (ZKP) mechanism in order to ensure the data's integrity and provide a secure means of data transfer. It establishes a connection with the Inter Planetary File System (IPFS), which is used for the purpose of storing data, and it makes use of Ethereum smart contracts for the purpose of securing data. When the data has been checked, it is included into the development of a deep learning architecture for the goal of safeguarding the integrity of the healthcare network and preventing unauthorized access. The Deep Sparse Auto Encoder (DSAE) and the Bidirectional Long Short-Term Memory are both elements that are combined in this design (BLSTM). The BDSDT has been shown, via testing performed on two distinct public data sources, to be superior to other solutions that are presently available on the market and to have an accuracy level that is very near to 99 %.

Uploading the data generated by Internet of Things devices to a data center has traditionally been done with the intention of training deep learning models. Despite this, there is a growing worry over the privacy of data, notably in the healthcare business, which is responsible for protecting personally identifiable health information. The concept of federated learning [15] describes an innovative strategy for solving this barrier. It is a method for training a shared global model by using decentralized data that is spread across various clients while simultaneously collaborating with a centralized server. Google is responsible for the development of this strategy. The purpose of this research is to offer a paradigm for the encrypted transport of data in healthcare IoT networks. The accomplishments of block chain-based data transfer models and the prospects of federated learning models as a means of enforcing security and privacy were the driving forces behind this line of study.

This article presents the Blockchain-enabled Federated Learning model for secured communication in the healthcare Internet of Things (BFL-hIoT), with the intention of ensuring the safety and confidentiality of healthcare data that is used in the training of deep learning models. The BFL-hIoT model was developed in order to meet the needs of the healthcare industry. Data is maintained disseminated in a secure way while employing the BFL-hIoT model, and the global model is educated via communication between clients and a centralized server. This strategy works within the context of the IoT in healthcare and aims to achieve a balance between two opposing demands, namely the protection of patients' privacy and the improvement of machine learning models. The outcomes of training and testing with this model on the ToN-IoT [16] dataset are compared to the outcomes of utilizing traditional methods. In comparison to the current state of the art, it has a high degree of precision and, in addition to normal behaviors, it is able to recognize nine unique types of assaults.

2. Related works

In their work [17,18], Zhang and colleagues present a blockchain-based secure data exchange system that is designed for use in an Internet of Things context. The authors propose a framework for the secure exchange of data that takes use of the advantages given by distributed ledger technology (blockchain) and internet of things technology (IoT). When it comes to the sharing of data inside the internet of things, the proposed framework provides assurances of non-repudiation, validity, and secrecy.

A secure Internet of Things environment is described in Ref. [19]. This ecosystem is founded on blockchain technology, and it increases the safety of data transmission and storage in the IoT. The authors utilize a technique called consensus to verify that the blockchain is trustworthy, and they use smart contracts to enforce security restrictions inside the IoT. The IoT might potentially benefit from the strategy that has been recommended in terms of maintaining data privacy, authenticity, and non-repudiation.

It is projected that unmanned aerial vehicles, often known as UAVs, would play a significant role in the expansion of cellular networks in the future. The sharing of spectrum between aerial and terrestrial communication systems will be a crucial component of these networks. The untrusted broadcast capabilities and wireless transmission that are present in UAV networks pose major dangers to an individual's safety and privacy, despite the fact that there may be certain benefits connected with using such networks. These risks may be outweighed by the potential benefits. Qiu et al. [20] present a one-of-a-kind solution for the safe trade and sharing of spectrum that protects users' privacy and is based on blockchain technology. The holes in the system's security that have been identified may be patched using their approach.

After that, Rathore et al. [21] presented a decentralized security architecture for smart city applications that combines SDN, fog computing, mobile edge computing, blockchain, and deep learning algorithms. This architecture was designed specifically for use with smart city applications. The use of a memory-hardened Proof of Work (PoW)

technique to authenticate Internet of Things devices is included into this architecture. This eliminates the possibility of a single point of failure occurring.

In a research that was somewhat comparable to this one, Wu et al. [22] addressed the problem of wasteful use of energy in blockchain-enabled cloud services and advised the usage of a hybrid cloud to solve the problem. When the blockchain has been installed in an edge device, such as a server or mobile device, it is then used as the foundation for the development of a cloud data center. The authors offered evidence to support their claim that combining blockchain technology with cloud computing resulted in increased operational effectiveness, greater data integrity, and increased flexibility.

Researchers Alsaedi et al. [23] highlight the significance of Intrusion Detection Systems (IDSs) for locating malicious activities in real-world applications that are able to circumvent security systems such as firewalls. According to their point of view, the evaluation of IDS approaches is highly significant, and the use of IoT-related datasets that accurately depict real-world scenarios is absolutely vital for the accurate and efficient evaluation of IoT security methods. After putting a number of machine learning and deep learning models through their paces, the researchers discovered that the Classification And Regression Trees (CART) model achieved the best level of accuracy (77 %), when it came to the classification of many classes of data.

The article [24] makes a suggestion for a Collaborative Intrusion Detection System (CIDS) that makes use of a Deep Blockchain Framework (DBF). In cloud-based environments, this approach is intended to detect cyberattacks while upholding users' constitutionally protected rights to personal privacy. Blockchain technology is coupled with a Trusted Execution Environment in this architecture in order to maintain the confidentiality of smart contracts. This hybrid solution provides this level of protection (TEE). In addition to that, this methodology guarantees that the availability and integrity of smart contracts will be preserved. In addition to that, the information gleaned from the network is encoded via the use of a deep learning model. This model has greater performance when compared to previous studies carried out in the same area and is resistant to assaults such as inference and poisoning.

A centralized controller oversees the operation of the software-defined industrial network to guarantee that there are no interruptions in the flow of data. This allows the network to operate as an autonomous ecosystem. In the paper [25], the authors describe a blockchain-based deep learning architecture that they've given the term BLockSDSec. This was done in order to overcome the problem. The safety of software-defined industrial networks is going to see an improvement as a result of this architecture. This framework makes use of a blockchain-based method that not only registers and verifies all of the switches using ZKP, but also validates them in the blockchain through a consensus process that is based on voting. In other words, this method not only registers and verifies all of the switches, but it also validates them in the blockchain.

Derhab et al. [26] introduced BMC-SDN, a security architecture that splits the network into different domains utilizing blockchain technology in combination with multicontroller software-defined networking. This study was conducted independently but was connected to the previous research. Blockchain technology is used to facilitate communication between the several master controllers that oversee the various domains that make up the SDN. These controllers are responsible for the management of each domain that makes up the SDN. The master controller is in charge of creating updates for network flows in the form of blocks, which are then authenticated by redundant controllers via an adaptive reputation mechanism. These blocks are the responsibility of the master controller.

According to our review of the relevant literature, despite the fact that there have been a great number of concepts proposed for securing IoT networks, the bulk of them exclusively target a certain category of security risk or a particular security mechanism. This is something that has been discovered as a result of the study that has been done. Few studies have been conducted on the application of blockchain technology in industrial networks, but those that have been done have concentrated on the benefits of combining blockchain technology with deep learning in order to develop solutions for IoT networks that are based on BCT. On the other hand, it is now abundantly obvious that even the most recent works do not satisfy the need for federated learning, which is required in IoT networks and is particularly crucial when it comes to the security of patient data in clinical settings. So, there is still room for development in the field of using blockchain technology with deep learning with the intention of enhancing security in healthcare IoT environments.

3. Materials and methods

This section describes the ToN-IoT dataset used in training and testing the model, blockchain architecture and the Federated learning model which form the basis of the proposed BFL-hIoT.

3.1. ToN-IoT dataset

The objective of the ToN-IoT dataset is to gather and investigate a wide range of data originating from sources related to the IoT and IIoT. It collects data from a broad number of sources and stores it in a variety of forms, such as telemetry data from connected devices, system logs from Windows and Linux, and network traffic. This data may be accessed in a variety of ways. This data was collected from a realistic network that included virtual computers, cloud layers, edge systems, and physical devices in a variety of permutations. The network was used to simulate real-world conditions. The major concentration of this dataset is on the subject of information security, with the overarching goal of determining the accuracy and usefulness of a wide range of cybersecurity solutions that are powered by artificial intelligence (AI). The ToN-IoT dataset contains records with a combined total of 43 characteristics, all of which are supplied in the CSV file format. Cross-Site Scripting (XSS), Distributed Denial-of-Service (DDoS), Denial of Service (DoS), Password Cracking, Reconnaissance or Verification, Man in the Middle (MITM), Ransomware, Backdoors, and Injection Attacks are the nine distinct types of attacks that are categorized according to these attributes. The dataset that was downloaded is outlined in Table 1, which may be seen here.

3.2. Blockchain structure

A blockchain is a kind of distributed ledger that records transactions over a network of computers. Blockchains are used in cryptocurrencies like bitcoin. Blockchain technology is used inside cryptocurrencies such as bitcoin. This specific kind of ledger does not have a centralized administration to oversee its operations. In the realm of cryptocurrencies, networks that make use of distributed ledger technology, more commonly referred to as blockchain, are utilized. This enormous number of nodes is what gives a blockchain network its fundamental framework and structure. A consensus technique is used to verify

Table 1
ToN-IoT dataset description.

Attack type	No of Records
Back doors	508,116
DoS	3,375,328
DDoS	508,116
Injection	452, 659
MITM	1052
Scanning	7,140,161
Ransomware	72,805
Password	1,718,568
XSS	21,089,844
Normal	796,380

transactions before they are added to a distributed ledger that is distributed in such a way that each node in the network has a copy of the ledger. A ledger is distributed in such a manner that each node in the network has a copy of it. Each and every node in the network is provided with a copy of the distributed ledger that is sent to them. Since the consensus technique ensures that every node in the network has the same version of the ledger, the ledger is particularly resistant to being altered or used fraudulently. This is because the consensus method assures that every node in the network has the same version of the ledger. This is due to the fact that every node in the network has an identical copy of the ledger.

Because of the way the chain is built, it is almost difficult to alter any of the previous transactions in the chain. The ledger's integrity is safeguarded inside a blockchain network by the use of cryptographic technologies. A chain of blocks that cannot be broken and that reliably records all network transactions is produced when, as shown in Fig. 1, each subsequent block in the chain is connected to the one that came before it through a hash. This creates a chain of blocks that cannot be broken and that produces a chain of blocks.

The structure of a blockchain network is decentralized, which means that rather than being administered by a single body, it is scattered over many nodes in the network. In contrast to this, a conventional network is characterized by its high degree of centralization. Every node in the network has a copy of the blockchain, and before any changes to the blockchain can be made, they must first be validated and authorized by the vast majority of the nodes in the network. This helps to ensure the integrity and security of the network, as well as prevent any malicious actors from making unauthorized changes to the blockchain. A blockchain of n blocks is represented as in equation (1), where each B_i is a block for $i \in [1, n]$ and t_i is corresponding timestamp.

$$BC := \{(B_1, t_1), (B_2, t_2), \cdots, (B_n, t_n)\} \tag{1}$$

To add a new block B_{new} to the existing blockchain BC, the following steps must be followed

1. A new transaction is validated and verified by the nodes in the network
2. The new transaction is added to the block B_{new} along with a timestamp t_{new}.
3. The block B_{new} is then added to BC by solving a cryptographic puzzle, such as the PoW
4. Once the puzzle is solved, the block B_{new} is broadcast to the entire network for validation and verification
5. Upon verification becomes a permanent part of BC.

3.3. Federated learning model

Federated learning is a decentralized machine learning technique, where instead of training the model on a central server with a large amount of data, the model is trained on many clients or devices that have access to their own local data. The clients work together to improve a shared global model, while keeping their data on their own devices and not sharing it with the central server. In this way, the privacy of the data is maintained while still being able to train a high-quality model. The central server aggregates the locally computed model updates from the clients to produce a global model, which is then sent back to the clients for the next round of training. The schematic of this model is shown in Fig. 2. The process continues until the desired accuracy is reached. Federated learning has been applied in various domains, including healthcare, finance, and mobile computing, where privacy and data security are important concerns.

A federated learning model M^t for classification can be represented as in (2) where M_i is the model at node i and F is the global consensus layer. M_i can be viewed as a local learner that learns M_i^t from the local

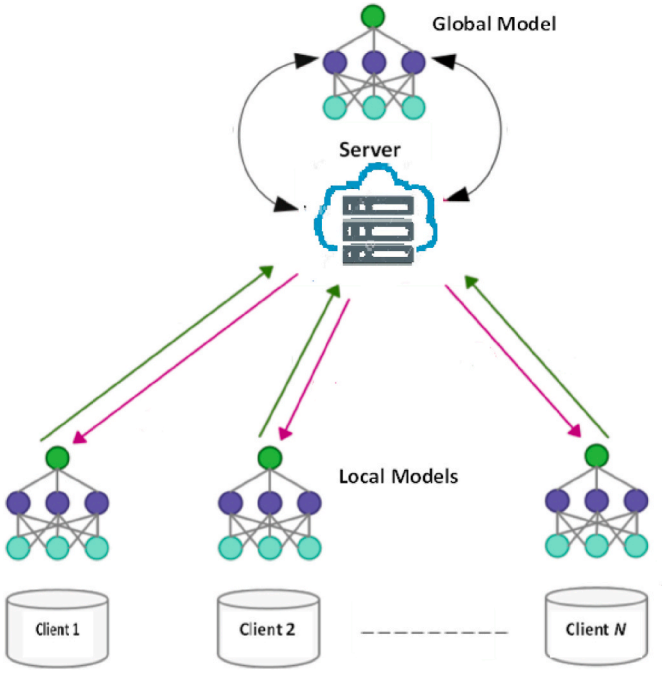

Fig. 2. Federated learning model.

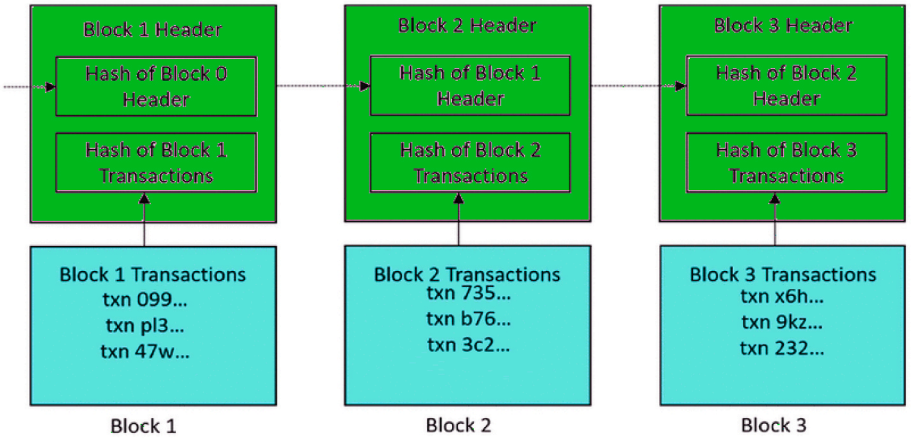

Fig. 1. Block chain structure.

dataset $\mathscr{D}_i$ and F is a fusion function that combines the local M_i^t models into a global model.

$$M^t = \left(\prod_{i=1}^{N} M_i\right) \otimes F, i = 1, \cdots, N \tag{2}$$

At the initial stage, the local model in each node is identical and the fusion function F only needs to learn the fusion parameters θ_F. Then the model parameters in the node i evolve as in (3). Once the global model is learned and the global learning is finished, the prediction of the model is the prediction of the local learner M_i^t, i.e., the model in each node is the best predictor.

$$M_i^{t+1} = \left(\prod_{j \in \mathscr{D}_i} M_j^{t+1}\right) \otimes F, i = 1, \cdots, N \tag{3}$$

4. Proposed blockchain enabled federated learning model

This research proposes the BFL-hIoT for ensuring privacy in the training of deep learning models with healthcare data in the healthcare IoT domain. With the BFL-hIoT model, data remains securely decentralized, and the global model is trained through communication between clients and a central server. This model aims to balance the need for privacy protection and the endeavors for improved machine learning models in healthcare IoT. BFL-hIoT is modeled as a multi-class classifier to discern normal users and abnormal users under nine types of attacks, by classifying the user data records and assigning target class labels. The BFL-hIoT model workflow is shown in Fig. 3. It is seen that the local modes are trained with IoT data captured at the clients are not shared across the network. The models are trained at the clients and the model parameters are exchanged between the cloud server through a decentralized blockchain.

4.1. Problem definition

This research formulates the federated learning model with N clients, where each client has its own dataset D_i and a local model $M_i, \forall i \in [1,N]$, and aims to learn a global model M_G by federating the local models in a scalable way. Formally, the global model is defined as in (4), where θ_G is a global model parameter and M_i defined in (5) is a local model parameter learned from D_i, for $\forall i \in [1,N]$, and M_i and M_j are independent from each other, and the global model M_G can be learned without any knowledge of the local model parameters M_i.

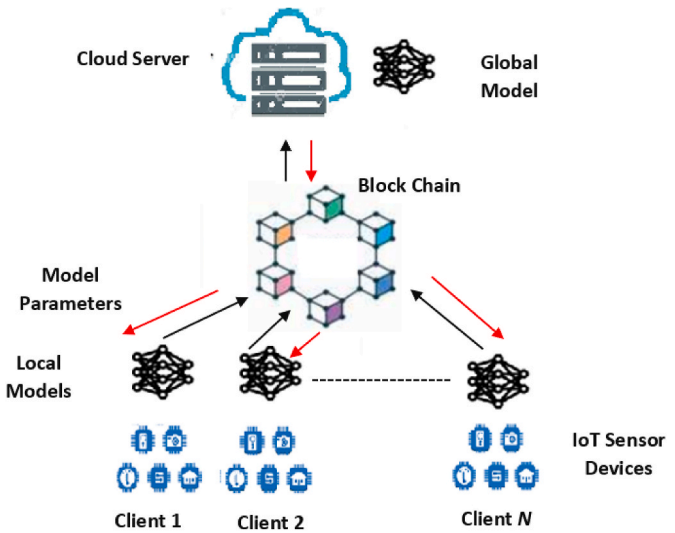

Fig. 3. BFL-hIoT model workflow.

$$M_G \triangleq \theta_G(M_1, M_2, \cdots, M_N) \tag{4}$$

$$M_i \triangleq \theta_i(M_1, M_2, \cdots, M_N) \tag{5}$$

Since the local models M_i are to be federated to the global model M_G, the federated learning model with each client i is defined as $M_{iG} \triangleq \theta_{iG}(M_i)$. Thus, the global model $M_G = \theta_G(M_1, M_2, \cdots, M_N) = \theta_{iG}(M_{1G}, M_{2G}, \cdots, M_{NG})$. In the federated learning model, each client i can access the global model parameters M_G by uploading its local model parameters M_{iG} to the cloud server; however, the cloud server is to keep local model parameters M_{iG} private and should not communicate M_{iG} to other clients. Thus, the local model parameters M_{iG} can be defined as the private data.

4.2. BFL-hIoT classifier

A deep learning classifier for the BFL-hIoT system is implemented using a BLSTM network. The architecture of a BLSTM network consists of multiple layers, including input, output, and hidden layers. The input layer receives the feature vectors x_i of the training records, and the output layer generates the predicted target labels $\acute{y}_i$. The hidden layers contain the memory cells and gates that process the input information and capture the dependencies between past and future inputs. The structure of the BLSTM is shown in Fig. 4.

The input data is fed into the first layer of the BLSTM network, where it is processed by the memory cells and gates in both forward and backward directions. This bidirectional processing allows the network to capture both past and future dependencies in the input sequence, resulting in improved performance compared to traditional Recurrent Neural Networks (RNNs). The processed information is then passed through multiple hidden layers, where the memory cells and gates continue to process the input data and propagate the information through the network.

Finally, the processed information is passed to the output layer, where a prediction is made for the target label $\acute{y}_i$ of each training record. The prediction is then compared to the actual target label y_i in the training dataset, and the error is used to update the model parameters through backpropagation. This process is repeated for each training record until the model has been trained on the entire training dataset. The trained model can then be used to classify new records and predict their target labels.

4.3. Blockchain enabled security mechanism

Blockchain enabled security architecture of BFL-hIoT is implemented with the following phases.

1. Data Encryption: The client data is encrypted using AES before sending it to the central server. This ensures that the data remains secure during transmission.

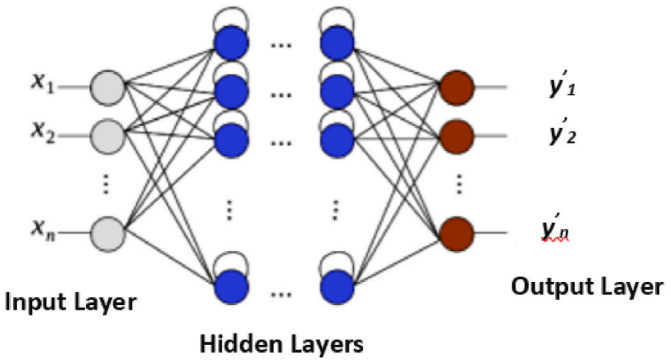

Fig. 4. BFL-hIoT model workflow.

2. Decentralized Storage: A blockchain network is used to store the client data in an encrypted form in a manner that is decentralized. This is accomplished using the blockchain protocol. This ensures that there is not a single point of failure centrally situated, and that the data will continue to be secure even in the event that an attack is made on the central server. Moreover, this eliminates the possibility of a single point of failure being the cause of several failures.
3. Blockchain Consensus: A consensus mechanism, such as Proof of Work or Proof of Stake, is used to verify that the data that is stored on a blockchain network is secure and cannot be changed in any manner. This may be done to ensure that the data is immutable. This eliminates any possibility of the data being taken without permission.
4. Access Control: The utilization of smart contracts, which indicate who may access the data and under what circumstances, is used in order to exercise control over who has access to the client's data. This is done in order to ensure that the client is satisfied with the level of protection afforded to their information. This ensures that only those persons who have been given authorization to see the data will have access to it.

The generalized verification process is described as below.

1. Data encryption: Let D be the data to be transmitted. The client C encrypts the data using a secure encryption algorithm E such that $E_{p_c}(D) = E_C(D)$, where p_c is the private key of the client
2. Hashing: The client C computes a hash of the encrypted data using a cryptographic hash function H such that $H(E_C(D)) = h$.
3. Transaction creation: The client C creates a transaction $T = \{E_C(D), h, p_S, s_C\}$ that includes $E_C(D)$, h, and other relevant information such as the recipient's public key p_S and the client's digital signature s_c.
4. Broadcasting: The client C broadcasts T to the blockchain network. The network nodes validate the transaction and add it to the blockchain.
5. Data retrieval: The server S retrieves the encrypted data from the blockchain using the transaction information and the recipient's private key k_S such that $E_S(D) = E_C(D)$.
6. Data decryption: The server S decrypts the data using the encryption algorithm and private key such that $D = E_S^{-1}(EC(D))$.
7. Hash verification: The server S computes a hash of the decrypted data and compares it to the hash included in T. If $H(D) = h$, the server knows that the data has not been tampered with during transit.

4.4. Model training

Given a training dataset $D_{Tr} = \{(x_i, y_i)\} i = 1, \cdots, n, y_i \in \{1,2,3,4,5,6,7,8,9\}$, where x_i is the feature vector of a training record, y_i is the target label, and n denotes the total number of records. This multi-class classification problem is modeled as a minimization problem as in (6) over a loss function L, with respect to the function $f : x_i \mapsto y_i$.

$$\min_{f,c} \sum_{i=1}^{n} L(f(x_i), c(x_i)) \tag{6}$$

The multi-class classification model is an arbitrary function $f(x)$, that assigns the target class labels for each x_i in D_{Tr} to generate a softmax classifier that assigns posterior probability p_i^k for each class $k = 1, \cdots, K$ (K is the number of classes). The classification problem is solved by minimizing the cross entropy loss, which is given as in (7). The softmax classifier is given as in (8). It assigns a posterior probability distribution over the K classes y to the input x, where the softmax loss for each class k can be interpreted as the cross entropy.

$$L(f(x), y) = -\sum_{K=1}^{K} \log p_K^K \tag{7}$$

$$p_k^k = \frac{e^{y_k}}{\sum_{k=1}^{K} e^{y_k}} \tag{8}$$

For a record of class k, the output will have a high value p_k^k and will be low for all other classes. The input x to the softmax classifier $f(x)$ is a collection of the user characteristics, that are concatenated into a fixed size vector. The classifier will assign $f(x) \in \{1, \cdots, K\}$ labels for the input x. Once $f(x)$ is found, it is converted into a class label through a function c. A cost function is then defined to assess the accuracy of the classifier $c(x)$ with respect to the ground-truth labels y as in (9), where $l(c(x_i), y_i)$ measures the divergence between the predicted label $c(x_i)$ and y_i as the cross entropy loss in (10), where $p_i^{y_i}$ is the posterior probability for class i predicted by the softmax function.

$$J(c) = \sum_{i=1}^{n} l(c(x_i), y_i) \tag{9}$$

$$l(c(x_i), y_i) = -\sum_{K=1}^{K} \log p_i^{y_i} \tag{10}$$

5. Experimental results and discussions

This section presents the experimental setup for running the proposed model, performance metrics employed, numerical results with illustrations and their interpretations.

5.1. Experimental setup

The efficacy of the BFL-hIoT model is measured using data collected from empirical studies. The hardware consists of an Intel Core i5 CPU, 128 gigabytes of random access memory (RAM), and the Ubuntu operating system. Python 3 and the PyTorch library are used throughout the development of the BFL-hIoT model. The Hyperledger Fabric is used to build up a public blockchain, and then smart contracts are authored and executed on a public Ethereum blockchain. The interfaces, such as the deep learning model interface, the blockchain interface, and the Byzantine Fault Tolerance (BFT) transaction interface, are all implemented as python modules. For training and testing purposes, the dataset is split in the proportion of 80:20 respectively. The data used for training are then split again, this time in a ratio of 70:30 for training and Validation. Table 2 contains the model's hyperparameters and their descriptions.

The use of hyperparameter tweaking in conjunction with grid search allows for these parameters to be optimized. A grid search technique is used in this method in order to test each and every conceivable combination of the candidate hyperparameters. This method involves defining a list of candidate hyperparameters for each parameter. The final hyperparameters for the model are determined by selecting the combination of variables that, when applied to a validation set, produces the best results.

Table 2
BFL-hIoT hyperparameters.

Hyperparameter	Value Range
Number of Hidden units	512
Number of LSTM Layers	3
Dropout Rate	0.1
Optimizer	Stochastic Gradient Descent (SGD)
Learning rate	0.001
Batch Size	128
Epochs	100

5.2. Evaluation metrics

For the purpose of evaluating the effectiveness of the model, the values of accuracy, precision, sensitivity, and specificity, in addition to the F1 value, are all taken into consideration. These values are obtained from the True Positive (TP), True Negative (TP), False Positive (FP), and False Negative (FN) values, as given in equations 11–15. One approach to thinking about accuracy is to consider it in terms of the percentage of correct classifications in relation to the total number of predictions made. A general classification's accuracy may be evaluated based on how effectively it was categorized as a whole. Specificity refers to the percentage of actual negative samples out of the total number of negative samples that are correctly identified, sensitivity refers to the percentage of actual positive samples out of the total number of positive samples that are correctly identified, and precision refers to the total number of positive samples out of the total number of positive samples detected by the model. The percentage of true positives that can be determined accurately out of the total number of samples that are considered positive is referred to as a test's sensitivity. The letter F1 represents the harmonic mean of the accuracy and recall, which is the same thing. These metrics range from 0 (inaccurate classification) to 1 (totally accurate classification) for each parameter on its own. 0 indicates an incorrect classification, while 1 indicates an accurate classification.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{11}$$

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

$$Sensitivity = \frac{TP}{TP + FN} \tag{13}$$

$$Specificity = \frac{TN}{TN + FP} \tag{14}$$

$$F1 = \frac{2\ Precision\ Recall}{Precision + Recall} \tag{15}$$

5.3. Performance metrics

The BFL-hIoT model is trained and validated with the respective data subsets and the accuracy and loss curves are illustrated with Fig. 5. It is seen that the models converge after 60 epochs (see Fig. 6).

The objective metrics of the model for the detection normal behaviour and nine attack categories are given in Table 3.

The results show that the BFL-hIoT model performs well on most categories with an average accuracy of 93 %. The highest accuracy of at 97 % was achieved in the Normal category while the lowest accuracy of 88 % was achieved for the detection of Ransomware. For most categories, the BFL-hIoT model achieved precision and sensitivity scores between 90 and 96 % and specificity scores between 93 and 98 %. The F1 Score, which is the harmonic mean of precision and sensitivity, was also in a similar range with scores between 88 and 96 %. In general, the results of the BFL-hIoT model are encouraging and demonstrate its effectiveness in detecting various types of network attacks.

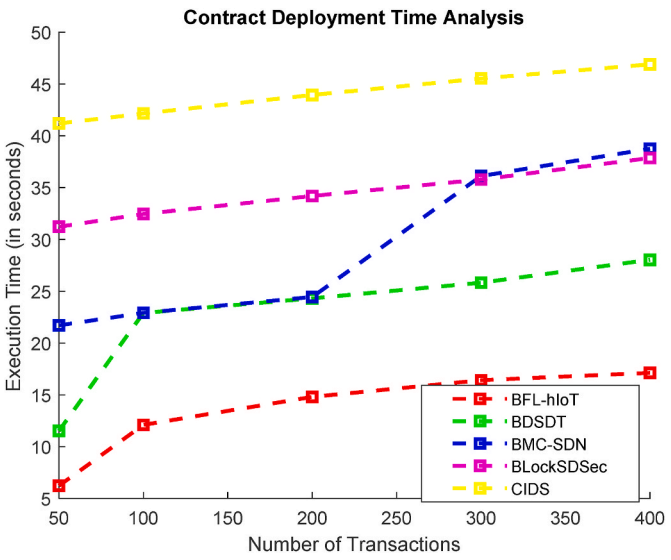

Fig. 6. Contract deployment time analysis.

Table 3
BFL-hIoT hyperparameters.

Category	Accuracy	Precision	Sensitivity	Specificity	F1 Score
Backdoor	0.9546	0.9631	0.9305	0.9817	0.9510
DDoS	0.9051	0.8901	0.8714	0.9035	0.8886
DoS	0.9404	0.9620	0.9164	0.9721	0.9432
Injection	0.9218	0.9378	0.9183	0.9429	0.9249
MITM	0.9031	0.9215	0.8707	0.9348	0.9039
Normal	**0.9716**	**0.9811**	**0.9619**	**0.9828**	**0.9781**
Password	0.9446	0.9545	0.9310	0.9611	0.9428
Ransomware	0.9288	0.9091	0.8621	0.9053	0.8842
Scanning	0.9210	0.9329	0.9017	0.9405	0.9292
XSS	0.9618	0.9732	0.9403	0.9129	0.9698

For a more comprehensive understanding of the performance of the BFL-hIoT model, it is compared with state-of-the-art models, evaluated with the same test data subset. Table 4 presents this data, which demonstrates the superiority of BFL-hIoT.

These results show that the proposed BFL-hIoT exhibits the highest classification accuracy of 0.9716 for normal behaviours and the lowest for MITM. The accuracy of this model is higher than that of BDSDT with a significant gain, for all kinds of attacks including normal behaviour. However, the CIDS, BLockSDSec and BMC-SDN lag behind these models

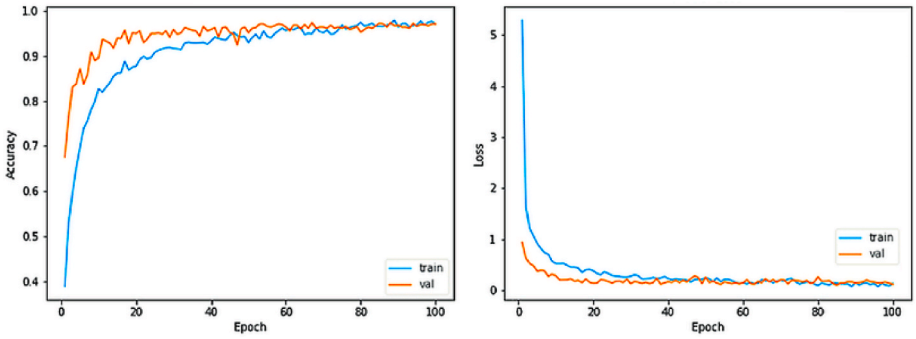

Fig. 5. Training and validation performance.

Table 4
Comparison of accuracy.

Category	Accuracy				
	CIDS [24] (2020)	BLockSDSec [25] (2020)	BMC-SDN [26] (2020)	BDSDT [14] (2023)	BFL-hIoT (Proposed)
Backdoor	0.8410	0.8939	0.8670	0.9215	0.9546
DDoS	0.7168	0.7942	0.7545	0.8821	0.9051
DoS	0.7656	0.8484	0.8059	0.8930	0.9404
Injection	0.7493	0.8303	0.7888	0.8740	0.9218
MITM	0.7331	0.8123	0.7716	0.8550	0.9031
Normal	0.7901	0.8754	0.8317	0.9215	0.9716
Password	0.7656	0.8484	0.8059	0.8930	0.9446
Ransomware	0.7168	0.7942	0.7545	0.8360	0.9288
Scanning	0.7493	0.8303	0.7888	0.8740	0.9210
XSS	0.7819	0.8664	0.8231	0.9601	0.9618

demonstrating lower detection accuracies under all categories. It is evident that the models are consistent with all categories. Further, it is seen that all the models detect Backdoor attacks with a high degree of accuracy which indicates that they are designed to capture the behaviour of adversaries trying to evade formal authentication mechanisms.

Further, the above models are compared based on the execution time taken for contract deployment with respect to the number of transactions. It is seen that the execution time increases with the number of transactions and BFL-IoT has the lowest execution time for all the transactions. This is attributed to the lightweight nature of BFL-IoT, while the rest are two-stage models.

Though the BDSDT is also based on BLSTM similar to the proposed BFL-hIoT, it uses a DSAE for latent feature representation before classification with BLSTM. It also employs a complex blockchain mechanism with a verifier and an exclusive server. The security of this model is at the expense of the blockchain architecture. On the other hand, BFL-hIoT leverages the federated learning and conventional blockchain approach in realizing the intended security mechanism. It poses the following advantages compared to the BDSDT model.

1. It has a high degree of scalability with the capability to include new clients, as the local models are trained independently at the local servers
2. The number of hidden layers of the DSAE employed with BDSDT adversely affect the performance of the model. BFL-hIoT relies on only the BLSTM for learning the features from the IoT traffic data.
3. While security of BDSDT is based on the blockchain architecture, the federated learning model and the blockchain complement each other in BFL-hIoT for achieving the security in IoT networks.

6. Conclusion

This research perceives the need for securing healthcare IoT data to avoid breaches of patient information and privacy in transmission. The proposed BFL-hIoT model uses a blockchain based smart contract for secure data transmission and federated learning to protect the privacy of patient data. The federated learning approach facilitates training the models by sharing the model parameters in a secured manner over the blockchain, protecting the data from unauthorized access. This model is validated and tested on the ToN-IoT set, which features a large collection of user records under normal user behaviour and nine classes of attacks. Empirical evaluations show that BFL-hIoT is superior to the state-of-the-art in attack detection and contract deployment. This model can be extended to address the issue of data heterogeneity in healthcare IoT networks, to ensure that it handle diverse data types and sources. BFL-hIoT can be integrated with existing security frameworks to create a more comprehensive mechanism to secure healthcare IoT networks.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] N. Scarpato, A. Pieroni, L. Di Nunzio, F. Fallucchi, E-health-IoT universe: a review, Management 21 (44) (2017) 46.
[2] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in: 2017 IEEE Technology & Engineering Management Conference (TEMSCON), IEEE, 2017, June, pp. 137–141.
[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, Security and privacy in the medical internet of things: a review, Secur. Commun. Network. (2018) 1–9, 2018.
[4] P. Nirmala, et al., An artificial intelligence enabled smart industrial automation system based on internet of things assistance, in: 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1–6, https://doi.org/10.1109/ACCAI53970.2022.9752651.
[5] R. Pavaiyarkarasi, et al., A productive feature selection criterion for bot-IoT recognition based on random forest algorithm, in: 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), 2022, pp. 539–545, https://doi.org/10.1109/CSNT54456.2022.9787583.
[6] M. Sugadev, S.J. Rayen, J. Harirajkumar, R. Rathi, G. Anitha, S. Ramesh, K. Ramaswamy, Implementation of combined machine learning with the Big data model in IoMT systems for the prediction of network resource consumption and improving the data delivery, Comput. Intell. Neurosci. (2022), 2022,pp 1-12.
[7] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Business & Information Systems Engineering 59 (2017) 183–187.
[8] R. Nowrozy, A.S.M. Kayes, P.A. Watters, M. Alazab, A. Ng, M.J.M. Chowdhury, O. Maruatona, A blockchain-based secure data sharing framework for healthcare, in: Blockchain for Cybersecurity and Privacy, CRC Press, 2020, pp. 219–241.
[9] D. Wood, N. Apthorpe, N. Feamster, Cleartext data transmissions in consumer iot medical devices, in: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, 2017, November, pp. 7–12.
[10] Y. Xie, J. Zhang, H. Wang, P. Liu, S. Liu, T. Huo, Z. Ye, Applications of blockchain in the medical field: narrative review, J. Med. Internet Res. 23 (10) (2021) e28613.
[11] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436–444.
[12] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, S. Andreescu, Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: opportunities and challenges, in: 2015 IEEE International Conference on Services Computing, IEEE, 2015, June, pp. 285–292.
[13] L. Hang, E. Choi, D.H. Kim, A novel EMR integrity management based on a medical blockchain platform in hospital, Electronics 8 (4) (2019) 467.
[14] P. Kumar, R. Kumar, G.P. Gupta, R. Tripathi, A. Jolfaei, A.N. Islam, A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system, J. Parallel Distr. Comput. 172 (2023) 69–83.
[15] T. Li, A.K. Sahu, A. Talwalkar, V. Smith, Federated learning: challenges, methods, and future directions, IEEE Signal Process. Mag. 37 (3) (2020) 50–60.
[16] T.M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, F.T. den Hartog, ToN_IoT: the role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets, IEEE Internet Things J. 9 (1) (2021) 485–496.
[17] M. Kamran, H.U. Khan, W. Nisar, M. Farooq, S.U. Rehman, Blockchain and internet of things: a bibliometric study, Comput. Electr. Eng. 81 (2020) 106525.
[18] W. Zhang, Z. Wu, G. Han, Y. Feng, L. Shu, Ldc: a lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications, Future Generat. Comput. Syst. 108 (2020) 574–582.
[19] M.U. Hassan, M.H. Rehmani, J. Chen, Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions, Future Generat. Comput. Syst. 97 (2019) 512–529.
[20] J. Qiu, D. Grace, G. Ding, J. Yao, Q. Wu, Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator's perspective, IEEE Internet Things J. 7 (1) (2019) 451–466.
[21] S. Rathore, B.W. Kwon, J.H. Park, BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network, J. Netw. Comput. Appl. 143 (2019) 167–177.
[22] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, M. Xu, EEDTO: an energy-efficient dynamic task offloading algorithm for blockchain-enabled IoT-edge-cloud orchestrated computing, IEEE Internet Things J. 8 (4) (2020) 2163–2176.
[23] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, A. Anwar, TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems, IEEE Access 8 (2020) 165130–165150.

[24] O. Alkadi, N. Moustafa, B. Turnbull, K.K.R. Choo, A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks, IEEE Internet Things J. 8 (12) (2020) 9463–9472.
[25] M. Singh, G.S. Aujla, A. Singh, N. Kumar, S. Garg, Deep-learning-based blockchain framework for secure software-defined industrial networks, IEEE Trans. Ind. Inf. 17 (1) (2020) 606–616.
[26] A. Derhab, M. Guerroumi, M. Belaoued, O. Cheikhrouhou, BMC-SDN: blockchain-based multicontroller architecture for secure software-defined networks, Wireless Commun. Mobile Comput. (2021) 1–12, 2021.