Internet of Things 15 (2021) 100422

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model

Saurabh Shukla[a,*], Subhasis Thakur[a], Shahid Hussain[a], John G. Breslin[a], Syed Muslim Jameel[b]

[a] Data Science Institute (DSI), National University of Ireland Galway (NUIG), Galway, Ireland
[b] Sir Syed University Engineering and Technology, Pakistan

ARTICLE INFO

Article history:
Received 30 November 2020
Revised 18 May 2021
Accepted 8 June 2021
Available online 29 June 2021

Keywords:
Healthcare
Internet-of-Things
fog computing
blockchain
cloud computing
edge computing
encryption
decryption
ring
symmetric key
asymmetric key
security
Diffie-Hellman
signature
cryptography

ABSTRACT

The healthcare Internet-of-Things (IoT) offers many benefits including data transmission in real-time mode, the ability to monitor the physiological state of the patient in a different interval of time. Devices such as blood-pressure monitors, glucose meters, heart monitoring implants, Electroencephalography (EEG), Electrocardiogram (ECG), and Electromyography (EMG) wearable devices allow health providers to collect the patient health information locally and make a real-time decision based on the Patient Health Data (PHD). Hospitals have been adopting the IoT for many years and now they have healthcare IoT devices in patients' rooms and their bodies. However, the medical agencies, hospitals, and companies do not consider the security risk of healthcare IoT devices connected to a Local Area Network (LAN) or Wide Area Network (WAN). The IoT devices can be easily hacked and may lead to several potentially life-threatening risks due to poor authentication and encryption practices. Existing machine learning algorithms and blockchain approach working in the cloud computing environment are unable to meet the Quality of Service (QoS) like reliability, authentication, identification, and security requirements of healthcare IoT devices. Most of the traditional machine learning algorithms and techniques for healthcare IoT lacks the real-world implementation for secure data transmission. Therefore, blockchain is introduced for secure and reliable transaction in healthcare IoT. Whereas Fog Computing (FC) is introduced to extend the services of the cloud at the edge of networks. Integration of FC with blockchain can overcome the issue of healthcare IoT device identification, authentication, and verification for scalable frequent data transmission in a decentralized environment. Hence, a novel solution for the abovementioned problem is proposed using FC and blockchain. It includes an FC-based three-tier architecture, an analytical model, a mathematical framework, and an Advanced Signature-Based Encryption (ASE) algorithm for healthcare IoT device identification, verification, and Patient Health Data (PHD) authentication. The aim is to extend secure data transmission for healthcare IoT and end-users availing the real-time services. The proposed model and algorithm will be able to provide services for transaction and transmission near the edge in a secure manner. By analyzing the generated results from the proposed novel ASE algorithm for throughput, packet error, reliability, and malicious node detection accuracy; it is observed that the ASE algorithm in the FC environment easily outperforms the cloud and the other

* Corresponding author.
E-mail address: saurabh.shukla@nuigalway.ie (S. Shukla).

https://doi.org/10.1016/j.iot.2021.100422

existing state of the art techniques such as FogBus, Femto cloud, Blockchain Fog-based Architecture Network (BFAN), and BeeKeeper. The malicious node detection accuracy of the ASE algorithm in the FC environment is 91% and in the cloud is 83%. Whereas the reliability percentage of the ASE algorithm in FC is 95% and in the cloud is 87%. The proposed approach is tested on simulators iFogSim (Net-Beans) and SimBlock.

1. . Introduction

Healthcare IoT market share will be around 39% of total IoT devices by 2025 [1]. Whereas the annual revenue for industrial applications of blockchain will be $19.9 billion by 2025, as per the report of Tractia an intelligent firm. IoTs are now enormously used in healthcare for facilitating the services to patients and doctors in real-time. Some of the healthcare time-sensitive applications such as ECG, EEG monitoring requires the constant evaluation of medical reports and Patient Health Data (PHD) [2, 3]. This all could be possible with the use of healthcare IoT devices in medical agencies and industries. However, the increase in the number of IoT devices and their increasing use has generated a large volume and veracity of data traffic. The handling of high IoT data traffic has become a major issue and concern using centralized features of cloud servers [4, 5]. This in return has increased the risks related to patient security and confidentiality. There will be a risk of patients' privacy exposure, data eavesdropping, ownership of medical health data, and location privacy. The intruders and hackers can now easily attack the IoT network by replication the data and changing the identity of healthcare IoT devices [6, 7]. Currently, the IoT-Cloud system is facing lots of challenges such as single point of failure due to centralized operation, malicious attacks, privacy leakage, and managing distributed IoT devices [8, 9]. The data transmission between healthcare IoT and cloud requires the trust, identification of devices, and authentication of users for network security and secure transmission of PHD.

Healthcare IoT has an inherent issue for capacity and scalability. Healthcare IoT generates gigabytes (GB) of healthcare data in real-time, this limitation represents a great barrier to its integration with blockchain [6, 10]. Moreover, the heterogeneity of healthcare IoT devices leads to a security issue in IoT networks. The protection and security of healthcare IoT data are directly linked to the identification of IoT devices. In case of no authentication, for example, attackers or intruders can hack the ECG IoT device and impersonate a real sensor and produce erroneous values. [11, 12]. Blockchain-based approaches involve significant energy, delay, and computational overhead not suitable for resource-constrained healthcare IoT devices [13-15].

To replicate the patient information among multiple fog nodes placed at the edge can be possible through a distributed ledger. Both blockchain and fog nodes operations are decentralized and distributed in nature [6, 16]. Both FC and blockchain have become fundamental techniques that result in the paradigm shift from centralized control to decentralized control. The patient confidential data can be recorded at different fog nodes using ledgers to provide transparency, security, and identity to IoT devices. FC nodes can be used for mining purpose in the hybrid model. Hence to overcome the issue of PHD authentication and identification of IoT devices in healthcare; FC plays a major role using the blockchain model by providing a distributed scalable network at the edge of IoT networks. Distributed FC nodes act as miners can collect the transaction information in blocks to check the validity. FC overcomes the limitation of high data traffic in healthcare IoT by minimizing the packet error during PHD transmission.

While blockchain can resolve and overcome the issue of security and privacy in IoT-FC-cloud system [17, 18]. Furthermore, blockchain technology is used to provide various cryptographic operations with mining at the edge of networks. The main advantage of using blockchain in the proposed model is that it keeps the records of PHD transactions by attaching timestamps to each block id along with the usage of different private keys and hash codes. Fog nodes in our proposed work are responsible for handling all possible communication between healthcare IoT devices to secure transaction between nodes and devices. Transmission of healthcare IoT requires a secure communication channel using decentralized blockchain technology and distributed FC approach. A signature scheme is used to ensure that the PHD is not modified during transmission from a healthcare IoT device to a fog node. Once the fog node verifies the PHD with a healthcare IoT digital signature and if the verification is conducted correctly, then it sends the acknowledgement/ response of the health data to the wearable IoT device. This process authenticates the PHD. Healthcare IoT devices are resources constrained devices, and with the increase in the number of IoT device; blockchain perform poorly. Therefore, to overcome this issue the IoT network is divided into several nodes and the PHD is distributed to different fog nodes. These fog nodes are spread over several clusters. Next, the storage of healthcare IoT data on the blockchain is not feasible therefore we have used fog nodes as they provide a safe platform with additional cryptographic security operations such as signatures and high advanced encryption algorithms [18, 19]. All the transactions are stored in different blocks and transferred to distributed fog networks. Diffie-Hellman key exchange technique and ring signature are used to transfer keys between healthcare IoT and fog nodes. The integration of the blockchain model at the edge of the network can provide reliable access and control over the healthcare IoT network. In

other words, there will be decentralized data storage via blockchain. The proposed intelligent FC-based blockchain model, a mathematical framework, and an algorithm are designed and developed to resolve the issue of healthcare IoT data authentication and IoT device identification for secure PHD transmission at the edge of networks.

2. Our Contributions

The principal aim of this research is the development of a novel approach to meet the QoS requirement related to security, authenticity, and reliability of Patient Health Data (PHD) transmission between healthcare IoT, fog nodes, patients (wearable device users), doctors, and the cloud servers using FC-based blockchain approach. To accomplish the main aim, the contributions of this paper are as follows:

- We proposed and designed a three-tier FC-based architecture for healthcare IoT in a blockchain platform to send secure and reliable data between IoT, fog nodes, patients, and doctors.
- Next, we developed a decentralized FC-based blockchain analytical model and a mathematical framework for secure data transmission and transaction in healthcare IoT. The model further performs identification, verification of certificates and keys for IoT devices and fog nodes using a private blockchain.
- We designed and developed a novel Advanced Signature-Based Encryption (ASE) algorithm. The algorithm performs the identification of heterogeneous and homogeneous healthcare IoT devices, verification of data sources and targets, and authentication of transmitted data via different IoT devices and fog nodes. The algorithm uses Diffie-Hellman (DF) key exchange method. The data is encrypted and then decrypted using a private blockchain and different cryptographic operations. The developed algorithm performs authentication of healthcare IoT devices using joint probability of IoT devices with random number generation. The proposed algorithm is a combination of four different algorithms.

3. Organization

The remainder of the paper is organized are as follows. An overview of blockchain and healthcare IoT with FC is given in Sec. 4. Sec. 5 briefly discuss the motivation and significance of the study. Sec. 6 introduces the system model and FC-based blockchain architecture. The methodology and the proposed work are discussed in Sec. 7 and Sec. 8. Sec 8. introduces the proposed system along with the ASE algorithm. Sec. 9 introduces the proposed analytical model along with its description. Whereas Sec. 10 discuss the mathematical framework for the proposed blockchain model. Sections 11 and 12 discuss the model implementation, experimental evaluation, results, and its setup. Finally, a short conclusion is given in Sec. 13.

4. Related Work

Currently, FC-based IoT is a hot topic. The previous papers did not include some major security aspects which are: (i) The data transferred from healthcare IoT devices to cloud servers are typically unencrypted and may get easily tampered with and attacked. This leads to a risk of releasing patient sensitive information (ii) To the best of our knowledge there is an urgency for healthcare IoT device identification which will lead to healthcare data verification and authentication this can conveniently be completed using blockchain in IoT-FC system [20]. In greater detail, servers should perform some authentication and verification in a decentralized manner at the edge of networks. In this section current techniques, approaches, and algorithms are discussed in detail related to healthcare IoT, fog, and cloud. These techniques mainly focused on security, reliability, cyber-attacks, IoT data authentication, and IoT device identification. Some of the existing works on blockchain and healthcare IoT security are summarized as follows:

In [21], LijinNg et.al proposed a novel system called BeeKeeper based on blockchain and IoT. In their proposed system a cloud server can process the data by performing computations on the user data. Any node can be a leader for server authorization which is elected by the present leader. They have used the Ethereum blockchain to deploy BeeKeeper. In [14], Somino et.al used different credentials by mixing private and public attributes. The users who own these attributes can use the credentials. The users here are the people using IoT devices. However, their proposed techniques are unable to perform the identification of IoT devices. They have used cryptographic operations with blockchain technique in IoT to minimize delay and network traffic. However, no work has been on the scalability issue of blockchain and IoT.

Similarly, in [15], Rahulamathavan et.al developed a partially centralized protocol. In this, the main authority was responsible for generating parameters for users and miners. The authors used encryption-based attributes so that they can be verified and decrypted by some specific miners and users who own the attributes. The technique was somehow helpful for IoT to maintain secure transmission. But their proposed work lacks the issue of device identification, authentication of keys. They mostly focus on secure transmission using a centralized manner. A distributed environment is absent.

In [22], the authors used blockchain for data integration and secure transmission. The unencrypted data are mostly stored in different locations at the receiving site following a peer-to-peer file storage protocol. They developed protocols for edge devices like FC which helps the end-users to process the data by maintaining integrity through blockchains. In [23], the consensus algorithm applications are explained in Proof-of-Work (PoW) blockchain models. In which miners find the solution to the given problem by distributing their computing powers. In [24], the authors presented an FC-based architecture using blockchain to improve latency and scalability in IoT networks. The architecture is an application to provide secure services to telehealth and tele-industries.

In [25], the authors proposed the integrated system of the blockchain with FC-based network architecture for Internet-of-Everything's (IoE). Furthermore, the FC nodes provide low latency and secure transmission to the smart city networks. In [26], the authors used blockchain for IoE in a decentralized manner. Which further makes the system tamper-proof. Moreover, it has reduced the maintenance, installation, and deployment cost. Their proposed system works well for IoE and smart cities which saves the devices from a man-in-the-middle attack. Furthermore, there are certain agreement and smart contracts for data transmission and transaction which are stored in Blockchain. In [27], authors Naveed Islam et.al proposed an FC-based framework using blockchain for healthcare applications such as recognition of patient activity. Their proposed framework categorizes and classifies the video frames based on patient activities using the Support Vector Machine (SVM) algorithm. However, the system does not fulfil the requirement of the identification of IoT devices in e-healthcare.

In [28], the authors proposed a blockchain-based architecture in the FC environment for IoE. It is a secured architecture that works in a fog-based network called Blockchain Fog-based Architecture Network (BFAN). Their proposed work utilizes blockchain for the security of data using various encryption and authentication techniques. The proposed architecture can be deployed in smart cities. The main aim of their proposed work is to minimize latency and energy consumption and to further improve secure data transmission using blockchain. Similarly, in [29], the authors Michael Harbert et.al proposed a plasma-based framework to overcome the issue of heavy load in blockchain when working for IoT. Their proposed framework is based on the concept of integrating FC with blockchain. In [7], the authors Muhammad Tahir et.al proposed a novel work for authentication and identification of IoT networks. Their proposed work consists of a blockchain-based IoT network that uses a probabilistic model and random numbers.

In [30], the authors proposed an infrastructure that works on the concept of Proof-of-Work (PoW). It is a lightweight infrastructure. The major function of the proposed model is to offload the computational task to fog and cloud using a consensus algorithm. They have used the Stackelberg algorithm which formulates the resource management at the fog nodes using a computational process. The optimization part is handled by the miners at the nodes. The purpose of service for offloading depends on the miners' interest. The model is verified and validated using the backward induction method. Whereas, in [31], the authors discussed various aspects and research challenges associated with the fusion of fog and cloud for latency minimization, resource allocation, secure transmission, optimization, energy consumption, and RAM usage in IoT. They expressed the problem of an increase in the number of heterogeneous devices and applications. In [32], the authors used the reinforcement learning algorithm with computation offloading of blocks, the approach works on a distributed environment where fog nodes are placed at the edge of IoT networks. However, their research work was unable to address the issue of security and privacy for data transmission between IoT, fog and cloud.

Similarly, in [4], the authors introduced a technique for data protection in centralized cloud servers from outside hackers. Their proposed technique is a combination of dynamic metadata and database schema design. They have used various cryptographic techniques in their algorithm. Future works require the implementation of the proposed work using a reinforcement learning algorithm. In [33], the authors applied the concept of binary ATM for a reduction in latency which further solves the problem of packet error in the cloud. Their results show that binary ATM is superior to conventional methods. Apart from this, node processing delays, which depend on the number of packets, are lower in binary ATMs when the component of constant bit rate (CBR) is equivalent to or lesser than variable bit rate (VBR).

However, in [34], the authors proposed the method of the Femto cloud. Their proposed method specifies a changing, self-configurable and multi-device mobile cloud from a group of mobile devices. This method enables many mobile devices to be arranged in integrated cloud computing servicing. The scheduler necessarily appoints duties using scheduling algorithm accessible tools to increase the available metrics while managing device churning. In [35], the authors proposed a framework called FogBus to minimize the data traffic by minimizing the network and CPU usage in IoT-Fog-Cloud infrastructure. Their proposed approach used a blockchain-based technique to minimize the high data traffic and secure the private confidential IoT data from outside intruders and hackers. It applies several encryption techniques to secure operations on IoT sensitive data. Also, the proposed framework facilitates the IoT-Fog (Edge)-Cloud infrastructure integration.

Similarly, in [36], the authors discussed the role of IoT for smart healthcare applications. Their discussion includes various technologies, several challenges, and opportunities associated with healthcare IoT, e-healthcare, and telemedicine. The authors further discussed the role of FC to minimize the high latency and meet QoS requirements for time-sensitive application in smart healthcare. They proposed a unique model to monitor patient health conditions. Next, the authors discussed the various wearable device to monitor and record patient vital signs. They used a machine learning approach in their system model.

In [37], the authors proposed a framework for a smart healthcare system using deep learning-based techniques to diagnose the patient heart disease in real-time mode by integrating IoT and FC. The framework was able to meet the QoS requirement for healthcare IoT. It was designed to operate for latency-sensitive applications like healthcare monitoring and flight control. Healthcare IoT generates a large amount of data called Big data. This data requires a large computation, next the data is transferred to databases and from databases to cloud data centres which lead to a drop in the performance of the system. Therefore, the proposed fog-enabled cloud framework meets the QoS for healthcare IoT in terms of power consumption, jitter, and prediction accuracy of heart disease diagnosis.

The existing IoE, IoT and medical devices work on a centralized model for communication. The IoT devices are validated by the cloud servers which in turn increase, the overhead related to cost for maintenance and infrastructure. Therefore, with the IoT device identity, the IoT data can be authenticated. Healthcare IoT device identification is important for authentica-

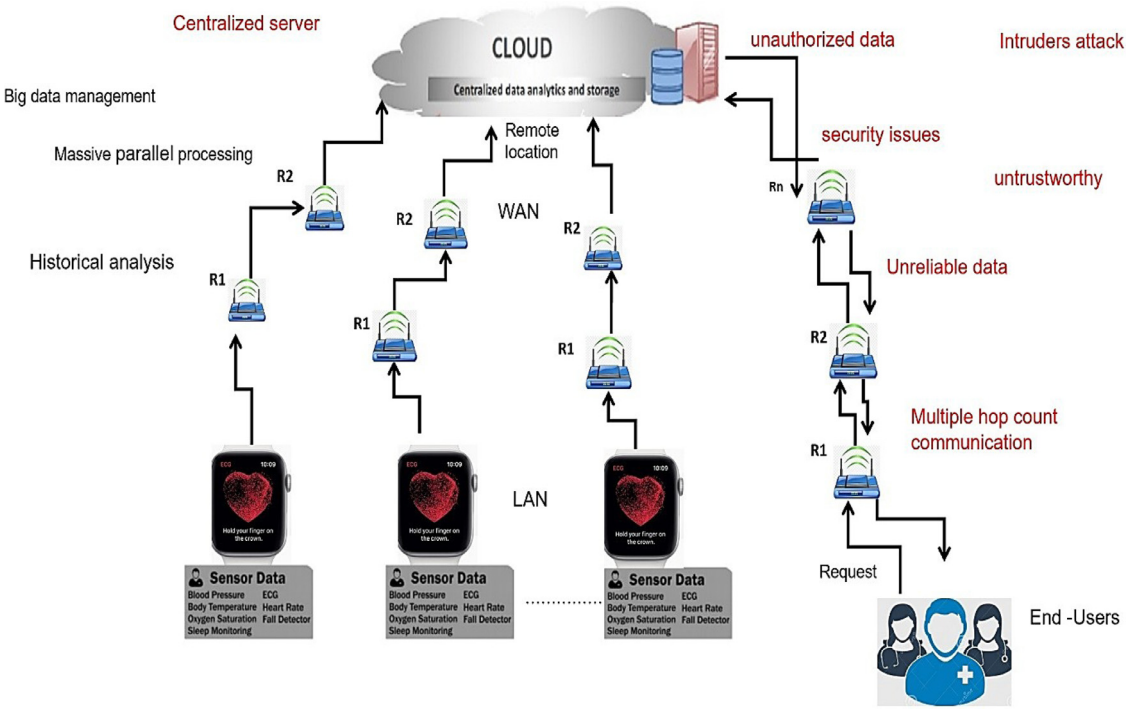

Fig. 1. Conventional healthcare IoT integrated model

tion and access control. This can be achieved using an integrated FC-based blockchain model which works in a distributed environment and decentralized manner. Where there is no single point of failure.

5. Motivation and Significance of the Study

This section discusses the conventional healthcare IoT data transmission with the cloud as a centralized server and the proposed enhanced data transmission model using the FC-based blockchain technique.

The main motivation for this study is the requirement of security, reliability, and authenticity for highly sensitive healthcare IoT applications. The fusion of blockchain and IoT with cloud computing working as a centralized server faces several challenges such as malicious node behaviour, packet errors, vulnerable codes in smart contracts, and unauthenticated IoT data. In the existing scenario, the trustworthiness of healthcare IoT data is of major concern for medical agencies. There can be tampered, alternation, falsified information in healthcare IoT through some intruders and hackers which may affect the end outcome of medical agencies, and hospitals.

In the medical healthcare IoT system, cloud servers have been used for storing, analyzing, and processing large data collected from IoT devices [24]. However, there are still three main challenges in healthcare IoT and cloud servers for secure data transmission such as 1) IoT device identification 2) Patient Health Data (PHD) authentication and 3) Verification of issued certificates and keys in a distributed environment [17]. In healthcare IoT data loss and error are intolerant. Healthcare IoT data is a high priority and sensitive data which needs to be updated every second [38]. The current existing algorithms, protocols, and analytical models for healthcare IoT are not designed to comprehensively address these issues simultaneously. They lack the PoW concept in healthcare IoT [39].

Most of the previous work for secure PHD transmission in healthcare IoT focused on heavy complex communication protocols and algorithms related to computation and memory requirements only [26]. They have faced a single point of failure due to a centralized cloud server. Therefore, healthcare IoT device identification and PHD authentication remain a challenging problem that has been not studied and discussed yet in healthcare IoT. The problem is worth meeting the QoS requirement for data transmission in healthcare IoT. Hence there is a scope to research this area. However, only a few studies have been conducted on it, but most of the recent research work lacks real-world implementation. See Figure 1 shows the conventional method of data transmission between healthcare IoTs and the cloud. Here R1, R2,….., ..Rn are the routers used in transmission.

Figure 1 shows the IoT-cloud environment that uses the multiple hop count for data transmission. All the conventional method deals only with data transmission using routers between IoT and cloud.

See Figure 2 for the advanced integrated FC-based blockchain model.

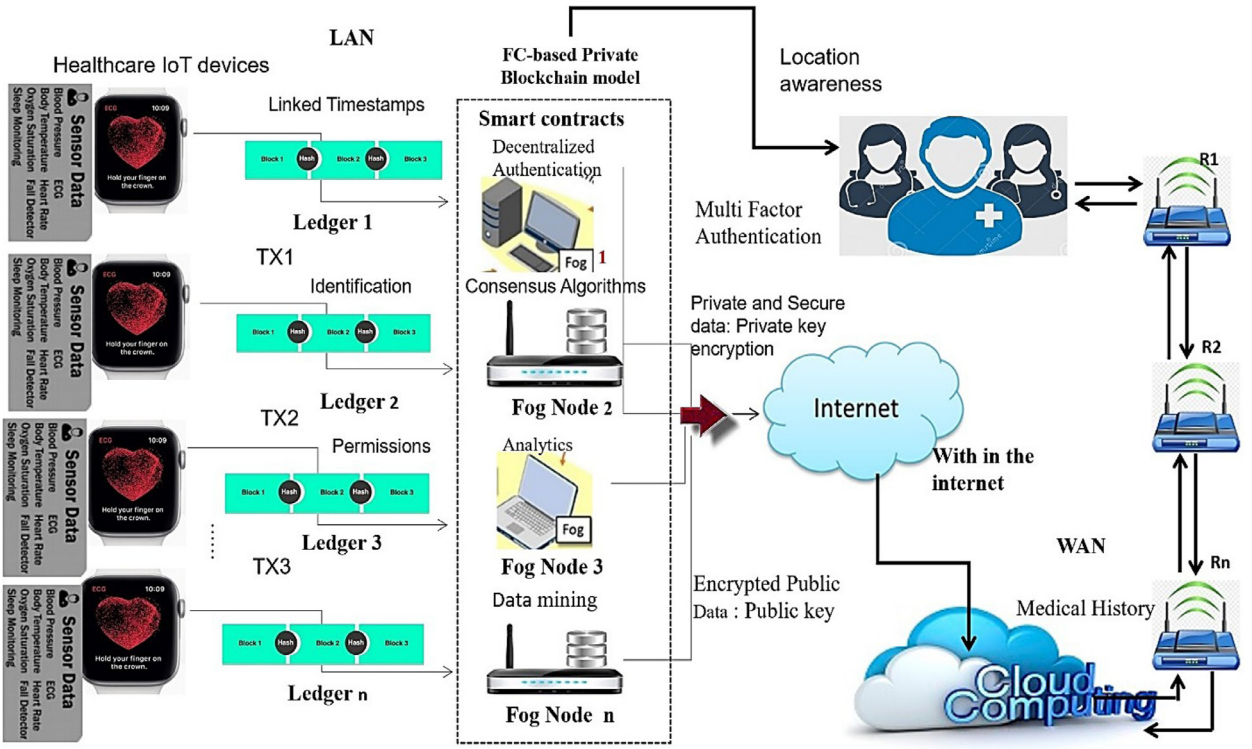

Fig. 2. Proposed integrated FC-based blockchain model

Figure 2 shows an enhanced data transmission method using an FC-based blockchain technique for secure data transmission in healthcare IoT and the cloud. Here R1, R2…...., Rn are the routers used in transmission. All the participating servers, nodes have the PHD and the means to verify that have not been tampered with this authenticity can be easily achieved. This method will guarantee data reliability and mining to be possible at the fog nodes with blockchain to operate in the FC environment. In this Figure 2, we have used the FC approach at the edge of networks. The time-sensitive healthcare IoT data is processed and filtered at the fog nodes. The fog node in this model is acting as a small sub-cloud server with limited storage and processing power. These fog nodes are easy to be deployed over a geographical region and can be distributed at the local hospital sites and medical agencies. When compares to cloud there is no single point of failure in FC.

Moreover, the FC technique is used in healthcare IoT to bring all the advanced features like resource sharing and server virtualization of the cloud near the network of IoT. The major benefits of using FC in our proposed system is that it minimizes service delay, network traffic and bandwidth consumption. In healthcare IoT, large data transmission of data leads to an increase in the network traffic which further increases the data packet error hence to overcome this limitation; FC plays a very major role in IoT networks. FC acts on the time-sensitive healthcare IoT data in milliseconds and the rest of the non-time-sensitive data it sends directly to the cloud for future storage and processing.

Whereas blockchain in the proposed system is used to overcome the issue of security, authenticity, identification, and detection of the malicious node along with packet error in healthcare IoT. Blockchain technology is used for storing the records of transactions between the different entities. It acts in a decentralized manner by keeping the information of every block id along with the attached timestamp.

The proposed FC-based technique could also be used and deployed for other secure operations and services in healthcare IoT. Such as e-healthcare, telehealth, telesurgery, telemedicine, remote-surgery, robot-surgery, ECG, EEG, and EMG data transmission, remote patient monitoring, and e-healthcare. Besides, the application of the work can be utilized in domains like Augmented Reality (AR) in healthcare which includes vein visualization and surgical visualization. Context-based augmented reality interaction and object guided tracking. The fog nodes can be deployed at the local hospital sites to collect the patient confidential data; while the historical data can be transferred to the cloud. The overhead related to communication cost, computation cost, bandwidth, and energy consumption cost will be reduced due to local deployment. This local deployment of fog nodes at the hospital sites will be a major boost in the current scenario of a pandemic like Covid-19.

6. System Model and Three Tier FC-based Blockchain Architecture

This section discusses the proposed three-tier FC-based blockchain architecture and system model for healthcare IoT using blockchain in the FC environment.

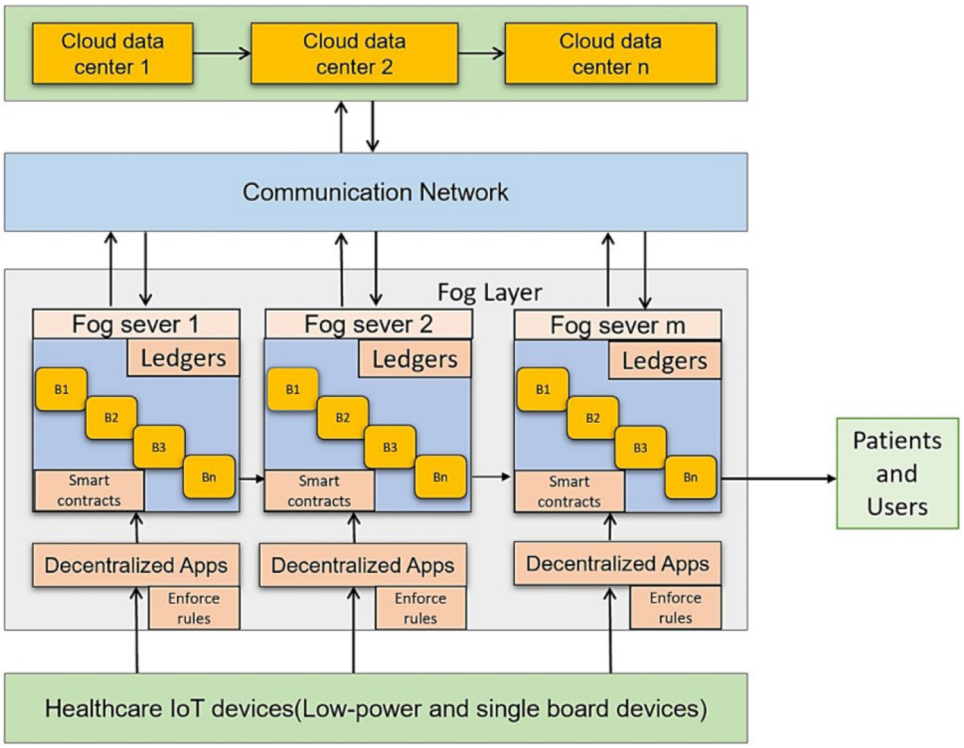

Fig. 3. Three-tier FC-based blockchain architecture

Figure 3 shows the proposed three-tier architecture where a fog layer is placed between the healthcare IoT devices layer and cloud data centres. The fog layer consists of multiple blocks, smart contracts written in a programming language and ledgers. Furthermore, the fog servers are connected to the healthcare IoT layer using decentralized Apps for distributed data processing. Patients and doctors can directly access the fog layer in the single-hop count. The main innovation of the proposed three-tier architecture is that it uses the concept of FC at the edge of healthcare IoT networks along with the blockchain technique using various cryptographic operations. The proposed architecture is used to design the system model for secure healthcare IoT communication along with authentication of healthcare IoT data and identification of IoT devices. Whereas the other state of the art techniques lacks the real-world implementation, development, and QoS requirement for healthcare IoT. The existing architecture and models are still in infancy when compares with the proposed three-tire FC-based blockchain architecture. However, the current analytical models and architectures such as Femto cloud, FogBus, BFAN, and BeeKeeper are not optimized for healthcare IoT requirement and could not address the above-mentioned issues. They are unable to provide a secure communication channel for time-sensitive healthcare IoT data transmission. See Figure 4 for the proposed healthcare IoT system model.

Figure 4 shows the FC-based blockchain system model for healthcare IoT. The data transmitted from healthcare IoT devices are first classified into confidential data and non-confidential data. Next, the healthcare IoT data is transferred to the fog layer which consists of fog servers where fog nodes using various cryptographic techniques perform data authorization and encryption. Fog nodes act as miners and collect the data in different blocks. Hashing is conducted using a healthcare IoT private key.

See Figure 5 shows the healthcare transaction process and sequence inside the FC-based blockchain model.

7. Methodology

The research passes through different activities to answer the research questions as shown in Figure 6. The activities are literature review, problem identification, design of three-tier architecture, development and implementation of the proposed ASE algorithm, development of FC-based blockchain analytical model, performance evaluation of the algorithm, simulation and analysis of the algorithm, demonstration and validation from healthcare data, benchmarking, and comparison with algorithm optimization.

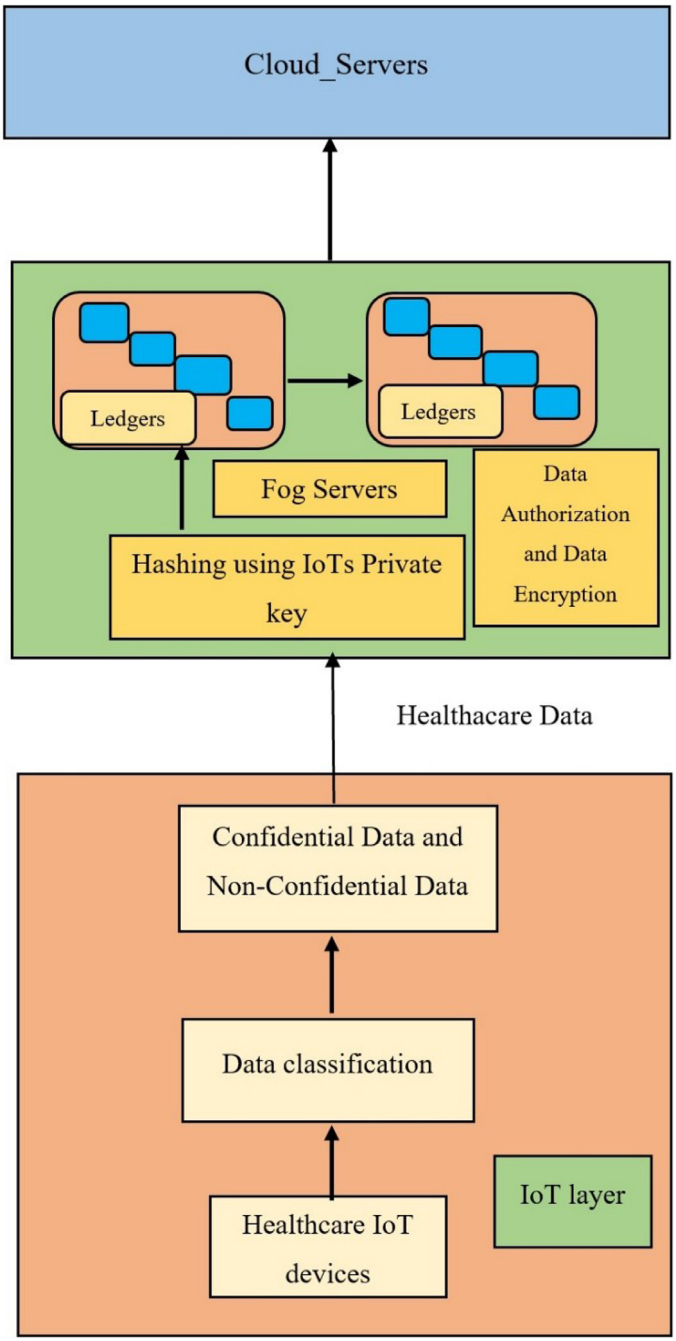

Fig. 4. The system model consists of Healthcare IoT layer, FC-based blockchain ledge layer, and cloud server

8. Proposed System

Our proposed system consists of healthcare IoT networks, FC storage, smart contracts, healthcare IoT devices i.e., the patient wearing devices, and doctors. Instead of storing healthcare IoT data over blockchains and cloud servers, we stored the healthcare data to the fog nodes and master fog servers. The fog storage arranges the PHD generated from healthcare IoT devices in similar blocks linked with a unique block. The fog nodes are attached to healthcare IoT. The network consists of fog nodes, healthcare IoT devices and they need to prove that the devices and data are authenticated with identification of devices, verification of certificates, and the exchange of keys.

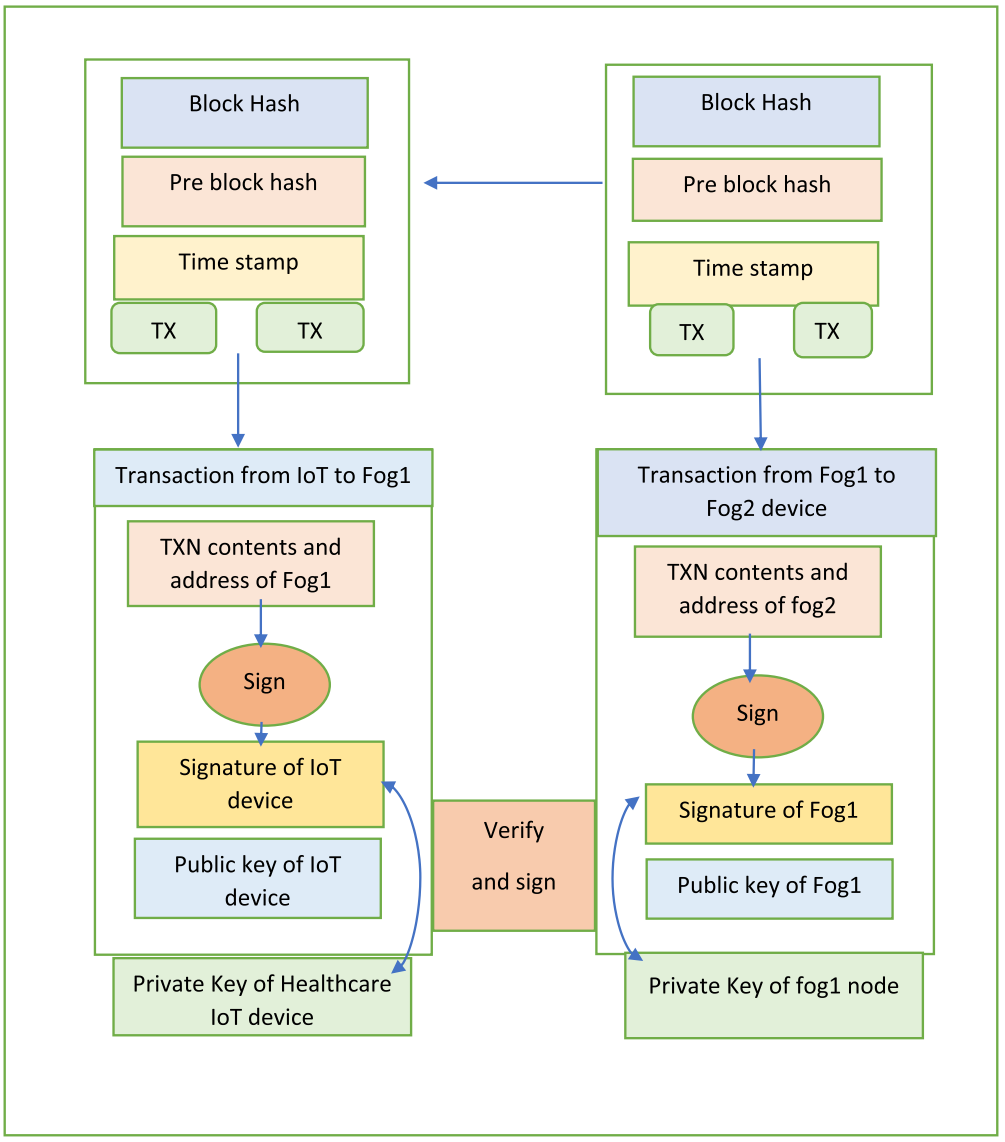

Figure 5. Healthcare IoT transaction process

After the completion of PHD data authentication and healthcare IoT devices identification; the transaction is proceeded with the signed data digitally using the ring signature. We have grouped the fog nodes into clusters. Each cluster has its master fog node with the public key. The fog nodes and master fog node exchange their roles from time to time based on the request of keys and transaction. Master fog node acting as a cluster head maintains the request made by the patients and users, they decide who can access the PHD of a healthcare IoT device. They also handle the request for PHD and key. In our system when a healthcare IoT devices want to send/transmit the PHD to a medical agency; the fog server verifies the transaction by a digital signature and sends it further to IoT networks along with the attached public address of the concerned doctor or medical agencies. The master fog node verifies the PHD signature and the healthcare IoT public key.

And if the public key is available the transaction of PHD file is broadcasted, if the key available then ok; else the PHD file is transacted to other nodes. In the case where the digital ring signature or the public key of any healthcare IoT device is not verified then the fog node will not broadcast healthcare IoT data to other fog nodes of the same cluster but transfer to other nodes. See Figure 7 for the digital signature description and sequence.

Fig. 8.

8.1. Advanced Signature-Based Encryption (ASE) algorithm

The proposed novel ASE algorithm consists of asymmetric cryptographic operations such as Diffie-Hellman key exchange and digital signature along with the usage of blockchain techniques. The digital signature in this algorithm consists of three

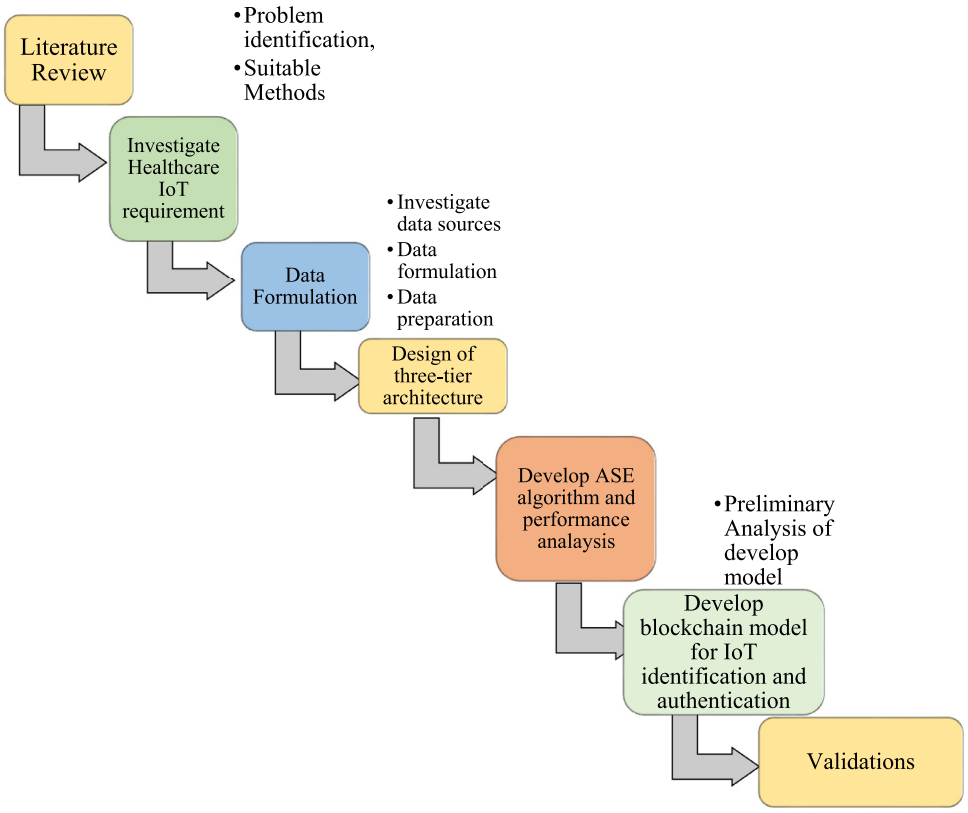

Fig. 6. Shows the research steps taken to achieve the objectives

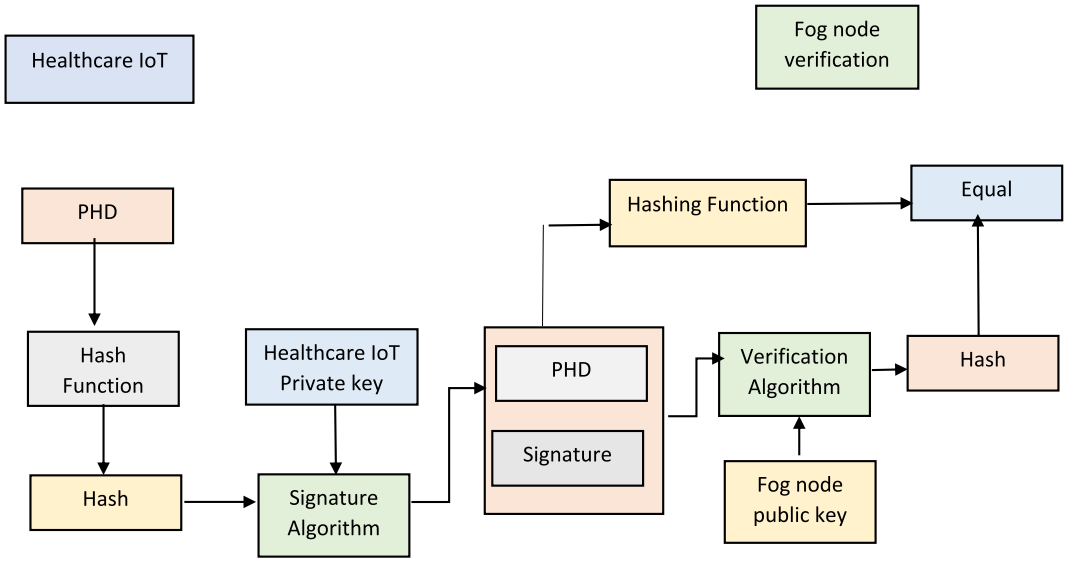

Fig. 7. Digital signature sequence

phases 1) Generation of keys 2) Generation of signature along with hash code and 3) Verification of signature. Furthermore, the signatures are mixed to form a ring. The algorithm uses the concept of FC for securely providing time-sensitive healthcare IoT data to patients and doctors. FC nodes act as miners for keeping the records of the transactions that occurred between IoT and end-users. Blockchain is used here in a decentralized way for data transmission in healthcare IoT.

Next, the algorithm is sub-divided into four major algorithms 1) PHD security using blockchain 2) Healthcare IoT data encryption using Diffie-Hellman method in blockchain 3) PHD decryption and 4) Healthcare IoT device identification, authen-

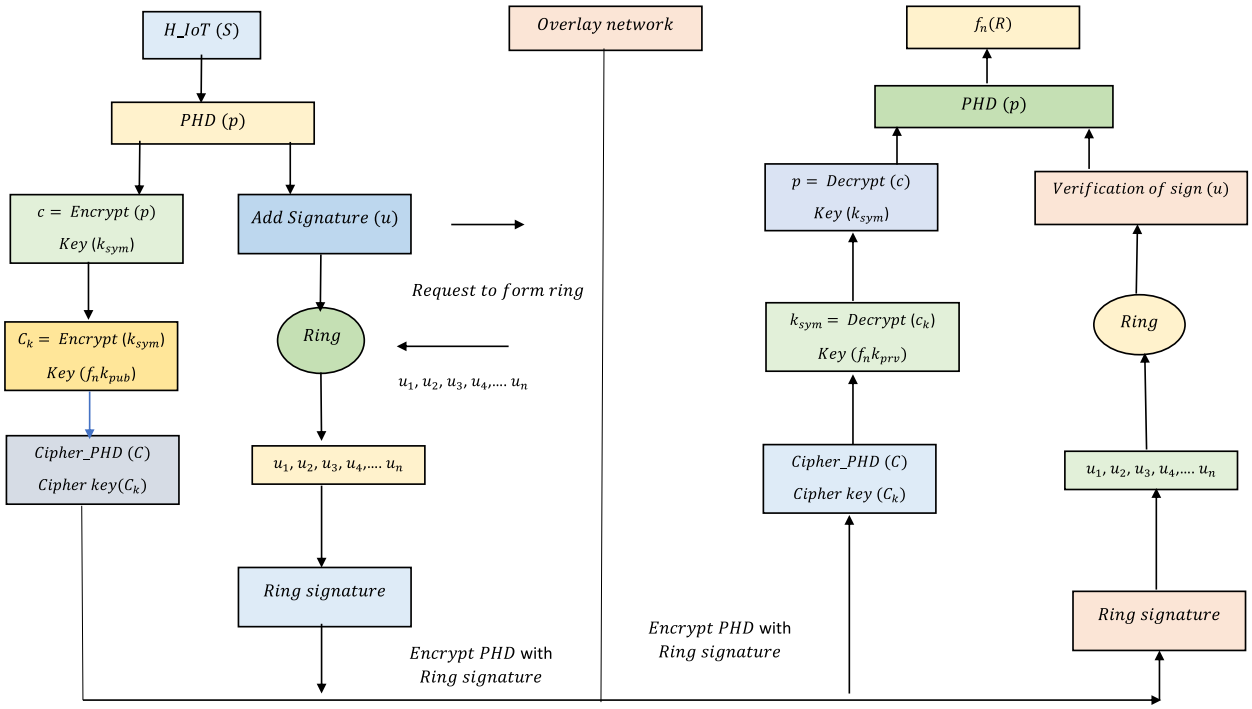

Fig. 8. Encryption and Decryption sequence model

tication, and verification for PHD transmission. The ASE algorithm can provide the secure transmission of PHD to end-users. Moreover, the proposed algorithm is expected to handle a large number of service requests from end-users or patients for healthcare IoT data. Additionally, this FC-based technique could also be used and deployed for other real-time operations and services in healthcare IoT.

The proposed ASE algorithm easily outperform the existing algorithms and techniques in terms of security and reliability of PHD. The existing state-of-the-art approaches are not able to fully utilize the concept of FC and blockchain at the edge of healthcare IoT devices. Therefore, they are unable to handle the time-sensitive healthcare IoT data. Most of the existing works lack the real-world implementation of the designed algorithms and models. The performance of the ASE algorithm is evaluated and compared with other existing algorithms in section 12.1 for malicious node detection accuracy and reliability. Algorithms 1–Algorithm 2Algorithm 3 and Algorithm 4.

9. Analytical Model Description

In the proposed model a certificate and a key are issued for fog nodes and healthcare IoT devices. The healthcare IoT data is retrieved using the keys. Certificates along with keys are verified using the proposed FC-based blockchain analytical model. The data is stored at the fog nodes. The healthcare IoT device sends an artificial key and PHD to the FC-based blockchain model. Certificates along with keys are verified using the proposed analytical model. Furthermore, the FC system formats PHD and send it to other fog nodes for further verification. The Interplanetary File System (IPFS) at fog nodes generates a hash code of data and send it to the blockchain network for mining to the respective miners.

Next, the three smart contracts are developed at fog nodes:

1 To check the status of miners.
2 To check the format of healthcare IoT data.
3 To verify the healthcare IoT users.

In our algorithm, we are using a symmetric key encryption technique. Our proposed algorithm is dedicated to securing both IoT-Fog networks and nodes from outside hackers and intruders. We further added a signature for the PHD authentication purpose. Due to the limitation of healthcare IoT devices a ring-based signature is used for the verification of certificates and keys. These signatures are used for PHD-file authentication. Each node sends a public-private key. Mostly, the key pairs used for signing and verification.

The keys used for encryption and decryption and different. In our case, the healthcare IoT has one key pair H_IoTk_{prv}, H_IoTk_{pub} and the fog nodes will have another key pair $f_n k_{prv}$, $f_n k_{pub}$. The healthcare IoT private key H_IoTk_{prv} is used to sign the PHD. While H_IoTk_{pub} key and H_IoTk_{prv} the key is used for verification and transaction. Healthcare IoT device feeds the data to $h =$ generate the hash value $Hash_{PHD}$.

Algorithm 1
Patient Healthcare Data (PHD) Security using Blockchain

Algorithm 1 performs security of PHD between healthcare IoT devices, fog nodes and end-users. It consists of patients, doctors, healthcare IoT devices, and fog nodes which uses an FC-based blockchain system for storing and securing the medical data. The users can then retrieve the data from these nodes. The output is the secured PHD. The algorithm further performs the healthcare IoT device request by different distributed fog nodes.

Algorithm Symbol Notation

P_{ax}: Patient
d_y: Doctors
H_IoT_z: Healthcare IoT devices
PHD: Patient Health Data
Data:
H_IoTID: ID of the interested healthcare IoT devices and healthcare ECG data.
R: The list of the configuration *H_IoT* devices sent by the fog nodes
Input: Patient = (P_{a1} , P_{a2} , P_{a3} ,----- P_{ax})
Doctors = (d_1 , d_2 , d_3 ,----d_y)
Healthcare IoT devices = (H_IoT_1 , H_IoT_2 , H_IoT_3 , H_IoT_z)
Output: Patient Healthcare Data (P_{ax} , H_IoT_z)
Successfully stored PHD in FC-based blockchain system
Algorithm Steps:
Step 1: FC-based blockchain system creation
Step 2: Patient selection
Step 3: Retrieve of PHD
Step 4: Assignment of doctor to healthcare IoT implant device
Step 5: Generation of healthcare IoT devices list
Step 6: Configuration of the healthcare IoT device

```
while Pax in Patient do
Select Pax
for each H_IoTz in IoT do
if the doctor d1 selects H_IoTz then
Retrieve PHD (Pax , H_IoTz);
Store In FC-based_Blockchain (Retrieved_PHD)
else
Select at least one patient;
end
end
end
function retrieve PHD (Pax , H_IoTz)
Pa1 = Pax from patient;
while H_IoTz in IoT do
if H_IoTz € Pa1 then
Retrieved PHD [] <- Pa1 . H_IoTz . retrieve value
get post. Val (PHD)
else
Assign Doctor for IoT implant to Pa1
goto retrieve PHD (Pax , H_IoTz)
end if
end
end
deviceList = queryAllDevicesInH_IoT (H_IoTID)
for ioTdevice in deviceList do for config in R do
if ioTdevice.DeviceID==config.DeviceID then
ioTdevice.status = con?g.request;
event(ioTdevice);
end if
config= R.next();
end
ioTdevice= deviceList.next();
end
```

A hash value of the PHD is the plain text and signature. H_IoTk_{prv} the key is then transferred to the proposed algorithm and send with encrypted PHD. During the verification process, the fog node verifies and generate the hash value and hash function of the PHD from the same hash function. Using the algorithm and the healthcare IoT public key extract the original hash value of the PHD and if the $hash\_P_{H\_IoT} = = hash\_C_{f_n}$ are similar then the data is verified and not forwarded during the transaction process. Next, to achieve the *H_IoT* anonymity and *H_IoT* correctness we have used digital ring structure. Healthcare IoT network is a collection of heterogeneous devices. Which allow *H_IoT* to sign the PHD in an anonymous key. This process helps in the identification of *H_IoT* devices.

The authentication process is performed at the healthcare IoT devices and fog nodes. Several messages are transferred between the nodes (i.e., healthcare IoT device, fog server, doctors, and patients). The fog nodes will now retrieve the data

Algorithm 2
Healthcare IoT Data Encryption using Diffie-Hellman Method in Blockchain.

Algorithm 2 performs the encryption of PHD over the blockchain. The PHD is generated from *H_IoT* and is encrypted using algorithm 2. The digital signature is designed using the Hash and private key. Asymmetric public-private key pairs are also used in the development of an algorithm. And at the last signatures are mixed to form a Ring. The algorithm uses the Diffie-Hellman method for the exchange of key among different healthcare IoT devices and nodes.

Algorithm Symbol Notations

PHD: Patient Health Data
K_{sym}: Symmetric key
K_{pub}: Public key
C: Ciphertext
C_K: Cipher key
f_n: Fog node
f_nK_{pub}: Fog node public key
SK_{pub}: Signed public key
SK_{priv}: Signed private key
H_IoT_PHD_File: Patient Health Data file generated from healthcare IoT
P_SIGNATURE: Patient signature
P_{ax}: Patient
$Encrypt_{sym}$: Symmetric encryption
$Encrypt_{asym}$: Asymmetric encryption

Algorithm Steps:

Step 1: Start the encryption process
Step 2: Generation of symmetric keys
Step 3: Next, generation of signature and use of Diffie-Hellman key exchanges.
Step 4: Generate the hash code
Step 5: Hash estimation
Step 6: Mix the signature to form a Ring

1: **Function** Encryption (*H_IoT_PHD_file*)
2: **if** Patient confirms PHD storage over blockchain then
3: Generate a symmetric key K_{sym}
4: $C < -Encrypt_{sym}$ (*H_IoT_PHD_File*, K_{sym})
5: $C_k < -Encrypt_{asym}$ (K_{sym}, f_nK_{pub})
6: **else**
7: do no operation
8: **end if**
9: **end function**
10: **Function** P_SIGNATURE (*H_IoT_PHD_File*)
11: **if** Patient chose anonymity over blockchain then
12: Generate a asymmetric public-private key pair (SK_{pub}, SK_{priv})
13: $Hash_p <$ - Estimate hash of *H_IoT_PHD_File*
14: Design the digital signature using the $Hash_p$and signed private key SK_{spriv}
15: Share the public key $SK_{pub}$to the $f_n$and receiver using Diffie-Hellman key exchanges
16: Mix the signature with other f_n and devices to form a ring
17: **end if**
18: **end function**

Algorithm 3
PHD Decryption

The algorithm performs the asymmetric decryption of PHD_ File using a fog node private key and a symmetric key.

Algorithm Symbol Notations

C: Ciphertext
C_k: Cipher key
f_nK_{prv}: Fog node private key
K_{sym}: Symmetric key
H_IoT_PHD_File: Patient health data file generated from healthcare IoT

Input: Encrypted *H_IoT_PHD_File*, ciphertext, cipher key, and encrypted symmetric key
Output: Decrypted *H_IoT_PHD_File*and K_{sym}

Algorithm Steps:

Step 1: Start the decryption process
Step 2: End of the decryption process

1: **function** *DECRYPTION* (C, C_k, f_nK_{prv}, K_{sym})
2: $K_{sym} < -Decryption_{asym}$ (C_k, f_nK_{prv})
3: *H_IoT_PHD_File*<- Decryption (C, K_{sym})
4: **end function**

Algorithm 4
Healthcare IoT Device Identification, Authentication and Verification for PHD Transmission.

Algorithm 4 performs the identification of healthcare IoT devices using FC and blockchain. The authentication and verification of issued certificates and private keys for healthcare IoT devices are conducted using random number generation and with joint probability formulation in the blockchain system. Each healthcare IoT device is uniquely identified by a "device ID" and the stored healthcare data. The mapping of device ID for healthcare IoT devices is conducted by fog nodes for device identification using a configured data stored on the blockchain.

Algorithm Symbol Notations

f_n: Fog node
H_IoT: Healthcare IoT device
f_s: Fog server
f_n: Fog node
D_A: Data allocation
T_S: Timestamp
C: Ciphertext
C_t: Certificate
C_S: Cloud server
d_y: Doctors
SK_{pub}: Signed public key
SK_{priv}: Signed private key
K : Key
$Hash_C$: Hash code
$Prvt_K$: Private key
$C_t\_H\_IoT$: Certificate linked with healthcare IoT
$C_t\_f_n$: Certificate linked with fog node
D_F: Data format
M: Miners
P_{ax}: Patient
$hash\_P_{H\_IoT}$: Hash code for the patient IoT device
$H\_IoT\_PHD\_File$: Patient Health Data file generated from healthcare IoT
$hash\_C_{f_n}$: Hash code for the fog node
$H\_IoT\_PHD\_File\_C$: Patient health data file C generated from healthcare IoT
H_IoT_PHD: Healthcare IoT PHD
S_C: Smart contracts

Algorithm Steps:

Requirement: f_n and H_IoT devices are present in the fog layer and healthcare IoT layer
Step 1: Classification of H_IoT_PHD
Step 2: Fog servers f_s consists of f_n to check for D_A.
Step 3: Next D_A at fog nodes using a private blockchain.
Step 4: f_n are used to store healthcare data
Step 5: f_n check the availability of free processor available at the f_s
Step 6: A timestamp T_S is attached to the block of data.
Step 7: H_IoT find the PHD to f_n using ledgers
Step 8: f_s allocates the PHD
Step 9: PHD authentication
Step 10: Mutual authentication of healthcare IoT devices
Step 11: Next to perform D_A and mining at the individual f_n.
Step 12: To issue a certificate C_t for f_n and H_IoT
Step 13: H_IoT sends a key and PHD to the f_s.
Step 14: Start of the verification process
Step 15: f_s verifies the C_t and key k
Step 16: Generate the $Hash_C$
Step 17: Next, send the $Hash_C$ to miners M
Step 18: Send Smart contracts S_C to f_n
Step 19: D_F checking
Step 20: M status is checked
Step 21: Verification of H_IoT and f_n
Step 22: Patient can use their own $Prvt_K$ to retrieve the H_IoT_PHD
Step 23: Use of Cipher identity suit to send the PHD
Step 24: At last, mutual Authentication at the fog nodes using comparison of the cipher identity key

Input: Encrypted $H\_IoT\_PHD\_File\_C$, Signers (fog node), and Signed Public key (SK_{Pub})

```
START
for each H_IoT device a C_t is issued
(FC-based blockchain system is created)
Data classification
if (PHD == Sensitive_Data) then
get geo-location and send the data for verification to f_n using SPARK
else if (PHD == non − sensitive)
then
H_IoT_PHD send to f_n to C_S
f_n allocates the PHD to f_s.
for each H_IOT_PHD do (H_IoT < −C_t)
C_t + T_S < - H_IoT_PHD
```

(*continued on next page*)

Algorithm 4 (*continued*)

```
if f_s== Available
 allocate the PHD
else no allocation
end if
end
function PHDAuthentication (H_IoT_PHD)
PHD _Retrieve(Prvt_k)
if C_t_H_IoT== C_t_f_n
 then
 Mutual Authentication (H_IoT_1, H_IoT_2, f_n, f_s, p_ax, d_y)
function VERIFICATION (C, SK_pub)
Hash_C<- calculate hash of the received encrypted H_IoT_PHD_File_Cto be verified
 Using Public Key SK_pubof H_IoT, extract Hash_pof H_IoTPHDfile
if hash_P_H_IoT == hash_C_f_n then
return C
else
return ''Signature incorrect''
end if
end function
```

through IPFS using the hash. Once the data is encrypted; it will be transferred to the blockchain network and from the blockchain network to patients and doctors. In the proposed system to change the contract of the state, i.e., to modify the blockchain, a transaction must be published in the network. The transaction is signed by healthcare IoT and must be accepted by the fog nodes and blockchain network. Every fog node creates a block, and the new fog node must verify the signature to confirm the ownership again. A ring signature scheme is used to mine the block in the blockchain network, in which the mined block is only considered as a valid block.

Signature here guarantees that the PHD information has not been modified and protected by a seal of proof such that its contents are not altered. The next encryption algorithm is used to encrypt the PHD generated from healthcare IoT using symmetric key encryption. To exchange the keys securely over cryptographic operations, we have used the Diffie-Hellman key exchange technique. The cipher identities are attached with *H_IoT_PHD_File* and sent from healthcare IoT device to fog nodes. And if the f_n at the receiver side possessed the information for cipher identity, then the mutual authentication is verified for homogeneous and heterogenous devices; or else it is not verified. Next, the communication channel is closed by ending the message with f_n identity. However, there are few assumptions have been made while designing the model. These assumptions are as first the patient can wear only one healthcare IoT device, next the patient will execute their smart contracts.

9.1. Authentication Method for Healthcare IoT Devices

The healthcare IoT devices are denoted as H_IoT_1, H_IoT_2, H_IoT_3, H_IoT_n. Where n is the number of IoT devices in the cluster. Each *H_IoT* has been given a number (H_IoT_i) for communication where $0 < i \leq m$. Now numbers N_1, N_2, N_3,—-, N_n are generated as authentication values. The function $N(.)$ is used to match healthcare IoT with corresponding numbers. The probability $P_{H\_IoT_a\, H\_IoT_b}$ ($H\_IoT_{a\ j}$, $H\_IoT_{b\ j}$) is calculated for two random variables H_IoT_a and H_IoT_b healthcare IoT device authentication. When $H\_IoT_a = H\_IoT_{a\ j}$ and $H\_IoT_b = H\_IoT_{b\ j}$. If a and b are matched, then they will become mutually authenticate. The two cases as described in section 9.1.1 and 9.1.2.

9.1.1. Probability for Similar Healthcare IoT Devices

In this case of similar functioning of healthcare IoT, the combined probability is evaluated in equation (1) and equation (2).

$$P_{H_{IoT\,a}\,H_{IoT\,b}}\left(H_{IoT_{a\,i}},\ H_{IoT\,b\,i}\right) = P_{H_{IoT\,a}}\left(H\_IoT_{a\ j}\right) P_{IoT_b}\left(H\_IoT_{b\ j}\right) \tag{1}$$

$$P_{H_{IoT\,a}\,H_{IoT\,b}}\ (1,\ 1) = P_{H_{IoT\,a}\,H_{IoT\,b}}\ (1,-1) = P_{H_{IoT\,a}\,H_{IoT\,b}}\ (-1,\ 1) = P_{H\_IoT_a\,H\_IoT_b}\ (-1,\ -1) = 1/4 \tag{2}$$

Generally, if H_IoT_a and H_IoT_b are n series; $n = 1, 2, 3, - - -n$ then equation (3) exists as

$$\sum_i \sum_j P_{H_{IoT\,a}\,H_{IoT\,b}}\left(H_{IoT_{a\ j}},\ H_{IoT\,b\ j}\right) = 1 \tag{3}$$

9.1.2. Probability for Different Healthcare IoT Devices

In the case of different types and functioning of healthcare IoT devices, the combined probability for H_IoT_a and H_IoT_b is shown in equation (4)

$$\sum_i P_{H\_IoT_a\,/H\_IoT_b}\left(H_{IoT_{a\ i}}/H_{IoT_{b\ i}}\right) = \sum_j P_{\frac{H_{IoT_b}}{H_{IoT_a}}}\left(H_{IoT_{b\ j}}/H_{IoT_{a\ j}}\right) = 1 \tag{4}$$

So, $\sum_i P_{H\_IoT_a\ /H\_IoT_b}\ (H\_IoT_{a\ i}/H\_IoT_{b\ i})$ shows the probability for union, where $H\_IoT_b\ = H\_IoT_{b\ i}$ holds true. The process when applied to its joint event j i.e. $\sum_j P_{H\_IoT_b\ /H\_IoT_a}\ (H\_IoT_{b\ j}/H\_IoT_{a\ i})$ that generates equation (5) and equation (6)

$$P\ (A\ \cap\ B)\ =\ P\ (A)\ P(B/A) \tag{5}$$

$$P_{H\_IoT_a\ /bH\_IoT_b}\ \left(H_{IoT_{a\ i}}/H_{IoT_{b\ j}}\right) = \sum_i P_{H\_IoT_a\ /H\_IoT_b}\ \left(H_{IoT_{a\ i}}/H_{IoT_{b\ j}}\right) = \sum_j P_{H\_IoT_b\ /H\_IoT_a}\left(H\_IoT_{b\ j}/H\_IoT_{a\ i}\right) \tag{6}$$

The heterogeneous healthcare IoT devices probability as shown in equation (7)

$$\begin{aligned}&\sum_i P_{H_{IoT_a}\ H_{IoT_b}}\left(H_{IoT_{a\ i}},\ H_{IoT_{b\ j}}\right) = \sum_i P_{H\_IoT_a\ /H\_IoT_b}\ \left(H_{IoT_{a\ i}}/H_{IoT_{b\ j}}\right)P_{H_{IoT_b}}\left(H_{IoT_{b\ j}}\right)\\ &= P_{H_{IoT_b}}\left(H_{IoT_{b\ j}}\right)\sum_i P_{\frac{H_{IoT_a}}{H_{IoT_b}}}\left(H_{IoT_{a\ i}}/H_{IoT_{b\ i}}\right) = P_{H\_IoT_b}\left(H\_IoT_{b\ j}\right)\end{aligned} \tag{7}$$

Next, equation (8),

$$P_{H_{IoT_a}}\left(H_{IoT_{a\ i}}\right) = \sum_j P_{H_{IoT_a}\ H_{IoT_b}}\ \left(H_{IoT_{a\ i}},\ H_{IoT_{b\ j}}\right) \tag{8}$$

Equations (7) and (8) are used for recognition during the healthcare IoT authentication process. Hence, healthcare IoT devices with different functioning in FC-based environment via probabilities $P_{H\_IoT_a}\ (H\_IoT_{a\ i})$ & $P_{H\_IoT_b}\ (H\_IoT_{b\ j})$ of the authentication information embedded in the smart contract.

10. Framework for Proposed Blockchain Model

Each fog node is assigned with the generated keys in the healthcare IoT model. The authorized PHD generated from the IoT devices are stored on the fog nodes using algorithm 1.

The two healthcare IoT devices H_IoT_A and H_IoT_B perform authentication as follows

Device H_IoT_A selects a number $R_{nH\_IoT_a}$ from a cluster as

$0 \le R_{na},\ 1 \le \log\ (id_{max/2})$ where $id_{max}$is the number length. The number and the healthcare message are encrypted with H_IoT_B a public key and transmit to H_IoT_B as denoted in step 1.

Step 1: $H\_IoT_A -> H\_IoT_B\ :\ 3_{H\_IoT_a}\ = (P_u K_b(H\_IoT_{A\ H\_IoT_a}\ ,\ R_{nH\_IoT_a}\ ,\ 1)$

The message 3_a receives at Healthcare IoT device A and decrypts to get the intended message.

Step 2: $3_{H\_IoT_a}\ ,\ R_{nH\_IoT_a}\ ,\ 1 <-\ D\ EP_r K_{H\_IoT_b}\ (3_{H\_IoT_a}\ )$
H_IoT_B selects a number $R_{nH\_IoT_b}$ enclosed as $0\ \le R_{nH\_IoT_b}\ \le id_{max/2}$
Step 3: $3_{H\_IoT_b}\ = EP_u(K_{H\_IoT_a}\ (R_{nH\_IoT_b}\ ,\ 1,\ H\_IoT_B\ \times R_{nH\_IoT_b}\ )$
Step 4: H_IoT_A decrypts the response received from H_IoT_B as
$R_{nH\_IoT_b}\ ,\ 3_{H\_IoT_b}\ <-\ DEP_r K_{H\_IoT_a}\ (3_{H\_IoT_b}\ )$

The acceptance is subjected to equality of $3_{H\_IoT_b}$ and $H\_IoT_B\ \times R_{nH\_IoT_b}$. If accepted, then H_IoT_A process the response and sends it to H_IoT_B.

Step 5: $3_{H\_IoT_c}\ = \mathrm{E}(P_u K_{H\_IoT_b}\ (H\_IoT_A\ ,\ R_{nH\_IoT_b}\ ,\ 1, R_{nH\_IoT_a}\ ,\ 2)$

Where $R_{nH\_IoT_a}$,2 is bounded by $0\ \le\ R_{nH\_IoT_a}\ <\ id_{max/2}$. H_IoT_A and H_IoT_B communicate until $(n\ -1)th$ message. H_IoT_A receives $(n-1)\ th$ message it decrypts and retrieves the information as follows:

Step 6: $(R_{nH\_IoT_a}\ ,\ H\_IoT_c\ ,\ 3_{H\_IoT_a\ H\_IoT_b}\ ,\ H\_IoT_c\ ) <-\ DEP_r K_{H\_IoT_a}\ (3(n-1))$

If $3_{H\_IoT_b\ ,H\_IoT_c}\ = H\_IoT_B\ \times H\_IoT_A\ ,\ R_{n,H\_IoT_a\ ,H\_IoT_c}$, So H_IoT_A calculates response 3_n and send to H_IoT_B as

Step 7: $3_n = \mathrm{E}(P_u K_{H\_IoT_b}\ (H\_IoT_A\ ,\ R_{nH\_IoT_a}\ ,\ \ H\_IoT_c\ ))$

Healthcare IoT device B decrypts the message and obtain information as

Step 8: $(3_{H\_IoT_a}\ ,\ H\_IoT_c\ +1,\ H\_IoT_d\ ) <-\mathrm{DE}P_r K_{H\_IoT_b}\ (3_n)$

Then check for

Step 9: $(3_{H\_IoT_a}\ ,\ H\_IoT_c\ +1) = (H\_IoT_A\ ,\ \ R_{nH\_IoT_b}\ ,\ \ H\_IoT_c\ )\&H\_IoT_d\ = 0$

Table 1
The hardware and software used for the implementation of the proposed model and algorithm

Hardware and Software	Specifications
Processor	Inter® Core™ i9-8750H
CPU	5.30 GHz
RAM	32GB
System Type	64-bit Windows 10
Platform	iFogSim, SimBlock, Spyder, and SPSS
Language	Java and Python

If the above conditions are true then the corresponding healthcare IoT devices are mutually verified, authenticated, and identified adequately or else decline. The analytical model is further verified using mathematical equations and implementing the algorithm. Furthermore, the substitution and elimination method of equation solving, and checking are also used to verify the proposed system accuracy.

The proposed system model is selected with the best skill. That is, the proposed model has the best-estimated skill when making predictions.

To orchestrate the message exchanged between the fog nodes and the healthcare IoT devices, we have proposed an application to perform operations and actions through blockchain. Each healthcare IoT device is uniquely identified by a "device ID" and the stored healthcare data. The mapping of device ID for healthcare IoT devices is conducted by fog nodes for device identification using a configured data stored on the blockchain. Let m be the total number of healthcare IoT devices C_k $(1 \leq K \leq m)$ be the configuration for the healthcare IoT device k, the transaction for IoT devices requested are described in Figure 9. It shows the sequence diagram for the collection of healthcare IoT data. The fog node composes the configuration requests $\{config\,1,\ config\,2 \ldots\ldots,\ config\,n$ for the healthcare IoT devices and sends the request to patients and doctors.

11. Model Implementation

In our proposed system, the healthcare IoT devices such as blood pressure monitor, ECG monitor are allowed to connect with the healthcare IoT network, PHD_file is sent to relevant smart contracts for analysis. If the health condition is abnormal, then the alert sent to the IoT-fog network and the doctors. PHD_file are stored to fog nodes and other distributed clusters. Healthcare IoT further participates to transfer the hash of the stored PHD to other fog nodes. The H_IoT adds a digital signature to the PHD. We have cryptographic techniques and operations from the proposed algorithm. Here H_IoT is treated as a sender and the fog node who is receiving the PHD_file could be treated as a receiver. Once the fog server/fog node gets information then they can access the full PHD_file as they have authorization over the network.

12. Experimental Evaluation and Setup

In this section, the execution of the proposed novel Advanced Signature-based Encryption algorithm (ASE) is evaluated and analyzed. The experimental evaluation is conducted in a real-time scenario for healthcare IoT. The performance of the FC-based Blockchain model that incorporates the proposed algorithm is analyzed through simulation and experiments. The baseline for this simulation is data authentication and healthcare IoT device identification for secure patient healthcare data transmission in an IoT-fog environment. To simulate the FC-based model, iFogSim as an open-source software tool, SimBlock for blockchain model implementation and the Python-based Spyder editor tool is used [40, 41]. The proposed ASE algorithm will be implemented in the iFogSim simulator [42]. The numerical simulation is conducted for the proposed platform is compared with the existing platform.

See Table 1 for software and hardware specifications

The algorithm is to be implemented using Netbeans and python with several main packages, modules, and classes.

12.1. Experimental Results

The general Healthcare IoT system consists of an IoT device, fog computing nodes, and clients. There are several inbuilt sensors in the healthcare IoT layer connected with the internet. The proposed FC-based blockchain analytical model and ASE algorithms are used to send the PHD to fog storage for further analysis. The healthcare IoT devices allow the patients and doctors to collect the PHD at regular intervals for different frequencies. A blockchain model is added for the reliability of the healthcare IoT-Fog system. At last, a real-time cryptographically secured PHD which is irreversible and immutable is retrieved. Patients can share now the PHD data to support medical research and innovations by getting identification of H_IoT devices in the Peer-2-Peer (P2P) network. iFogSim simulator is used for the experimental of the proposed model and algorithm. The fog node communication is connected through the Giga ethernet. The incoming PHD are processed at the fog nodes. The experimentations are performed for 1200 seconds in simulation. We set the idle CPU power at 100 watt and maximum power at 150 watts. We developed a PoW implementation for the IoT-Fog system, Ethereum was chosen as

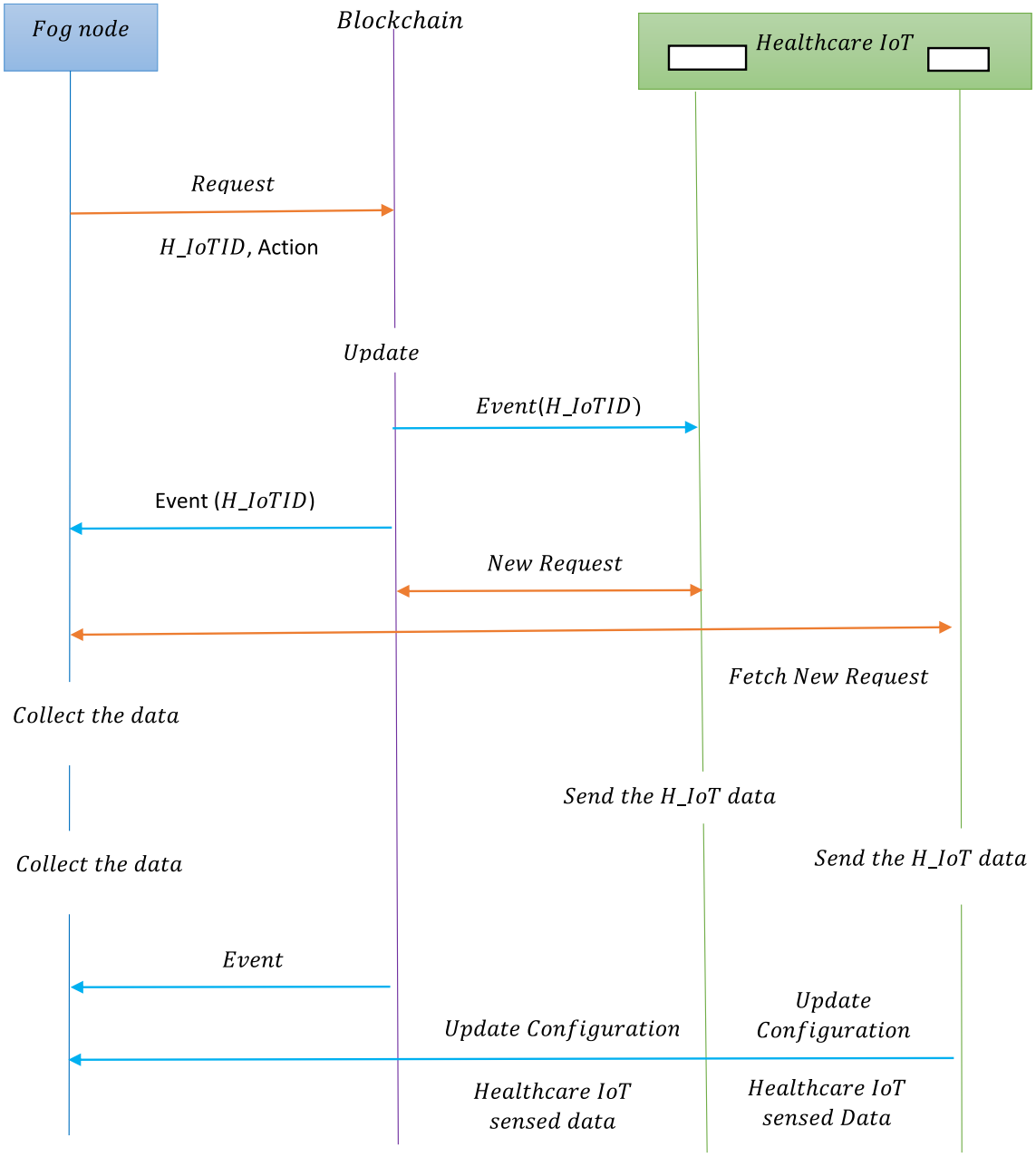

Fig. 9. Healthcare IoT data collection sequence

the blockchain-based technology for PoW. Next, the Profiler of NetBeans IDE 8.1 act as performance analysis tools for our proposed model and algorithm in simulation. We analyze the performance of our algorithms used in Ethereum as PoW in terms of CPU time and memory.

We presented a security analysis of the proposed architecture. Furthermore, this section discusses the details of the iFogSim simulator settings for the proposed algorithm implementation. See Figures 10-14 for the graphical user interface (GUI) built-in iFogSim [42, 43]. The Figures represent physical topology configurations from configuration 1- configuration 5. These configurations will help in the future to get the preliminary idea of real-world implementation and deployment of the healthcare IoT-FC-cloud system. The ECG health data is taken as an input value to the proposed system model [44, 45]. The ECG requires real-time monitoring of fewer than 300 milliseconds for one-way real-time data transmission. Whereas a certain application may tolerate less than 1 second for end-to-end ECG data transmission. In ECG data loss and error are intolerant. It is a high priority and sensitive data which needs to be updated every second.

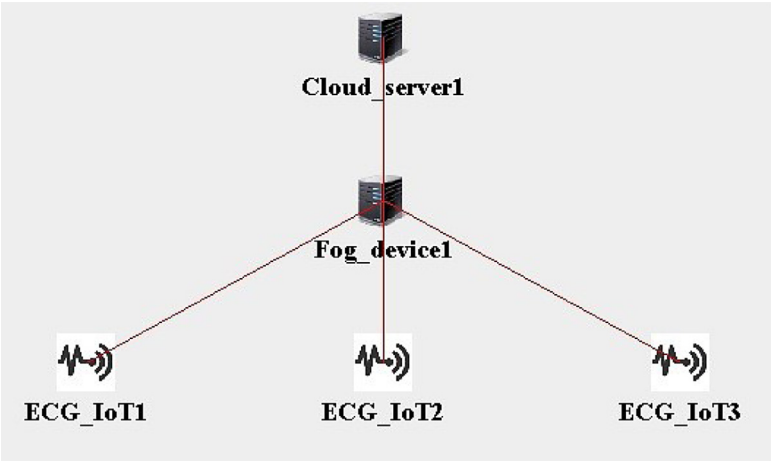

Fig. 10. GUI configuration 1

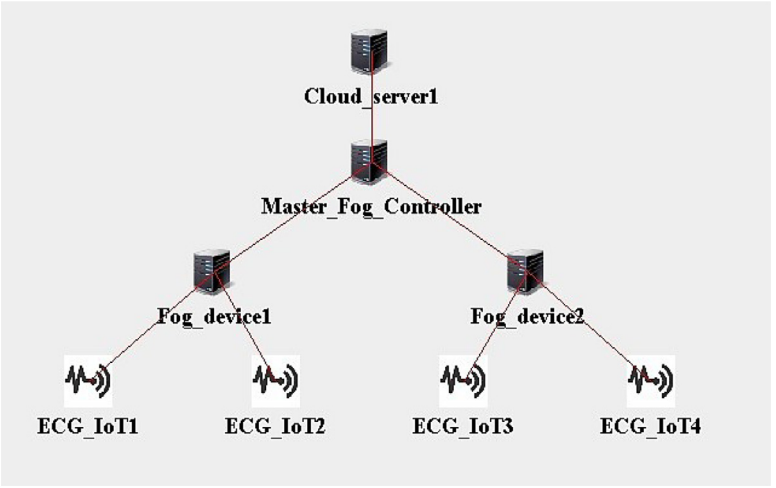

Fig. 11. GUI configuration 2

Table 2
Fog device description

Device Type	CPU (GHz)	RAM (GB)
Fog_device1(Mobile device)	2.6	2
Fog_device2(Mobile device)	2.6	2
Master_Fog_Controller	3	3
Cloud_server1	4	4

Figure 10 shows the physical topology for configuration 1 built-in the iFogSim simulator [42, 43]. Configuration 1 is solely based on the concept of a proposed system. Three ECG IoT devices are used in Figure 10 to send the healthcare data to the fog device.

Configuration 2 in Figure 11 consists of 4 ECG IoT devices. These ECG devices transmit the classified PHD to Fog_device1 and Fog_device2.

Configuration 3 in Figure 12 consists of 5 ECG IoT devices. These ECG devices transmit the classified PHD to Fog_device1 and Fog_device2.

Figure 13 consists of 6 ECG IoT devices. These IoT devices transmit the classified PHD to Fog_device1 and Fog_device2.

A total of 7 ECG_IoT devices are used in configuration 5 for PHD transmission to fog nodes. The 4 ECG_IoT devices transmit the data to Fog_device1 and 3 IoT devices transmit the data to Fog_device2.

See Figures 15 and 16 show the total time of execution and garbage collection along with heap used in fog nodes.

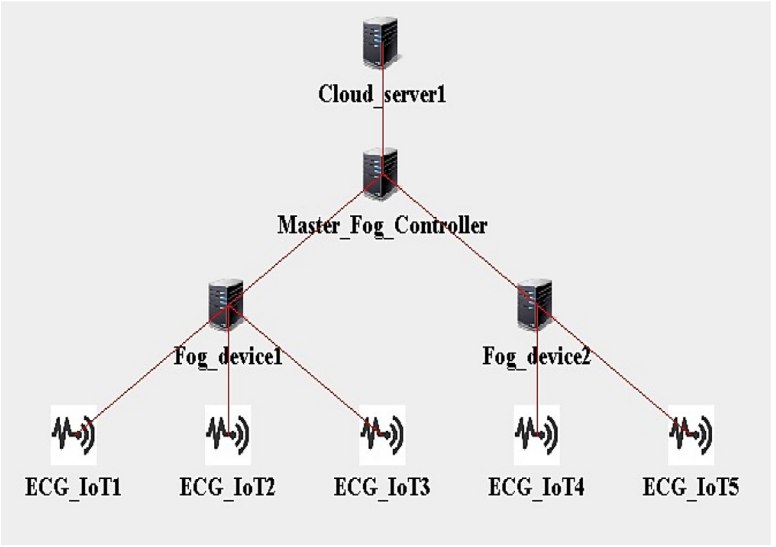

Fig. 12. GUI configuration 3

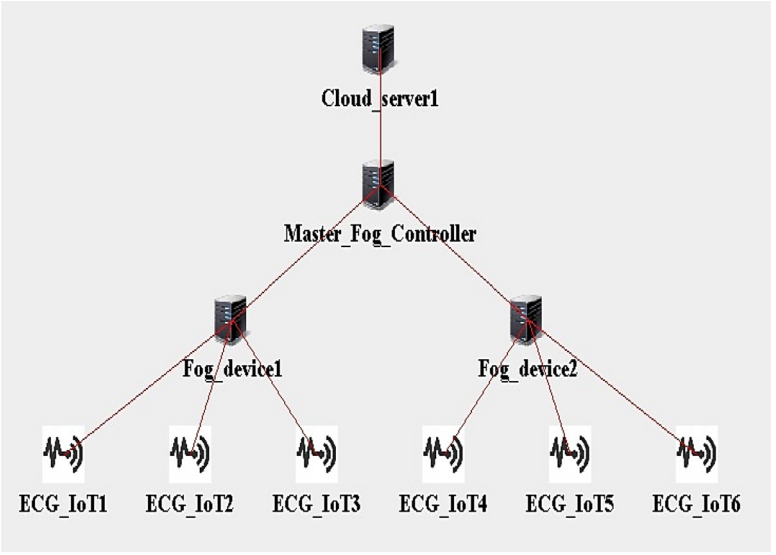

Fig. 13. GUI configuration 4

Table 3
Edge Module description

Tuple Types	CPU Length (MIPS)	Network Length(bytes)
Raw data (ECG) stream	1200	2100
The patient health data stream	2200	1700
Time-sensitive data stream (Real-time)	2800	1700

Table 4
ECG sensor configuration

CPU Length	Network Length in bytes	Data packet average arrival time at different intervals(ms)
1200 Million instructions	22000 bytes	25 milliseconds

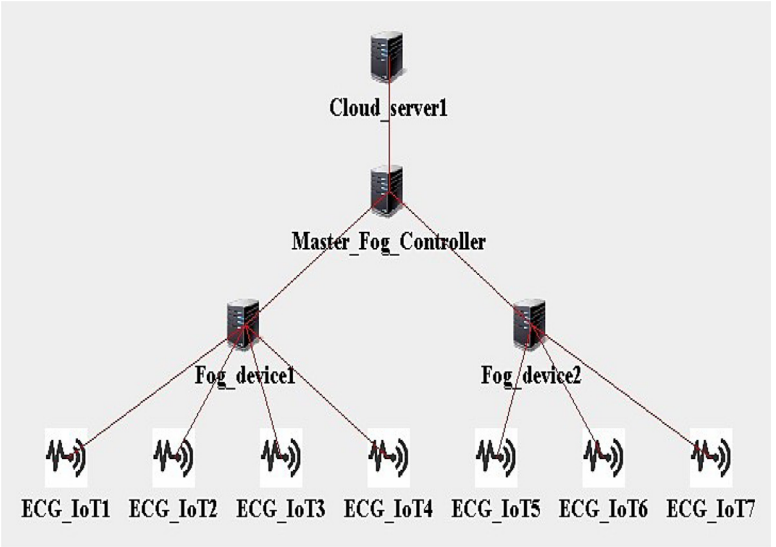

Fig. 14. GUI configuration 5

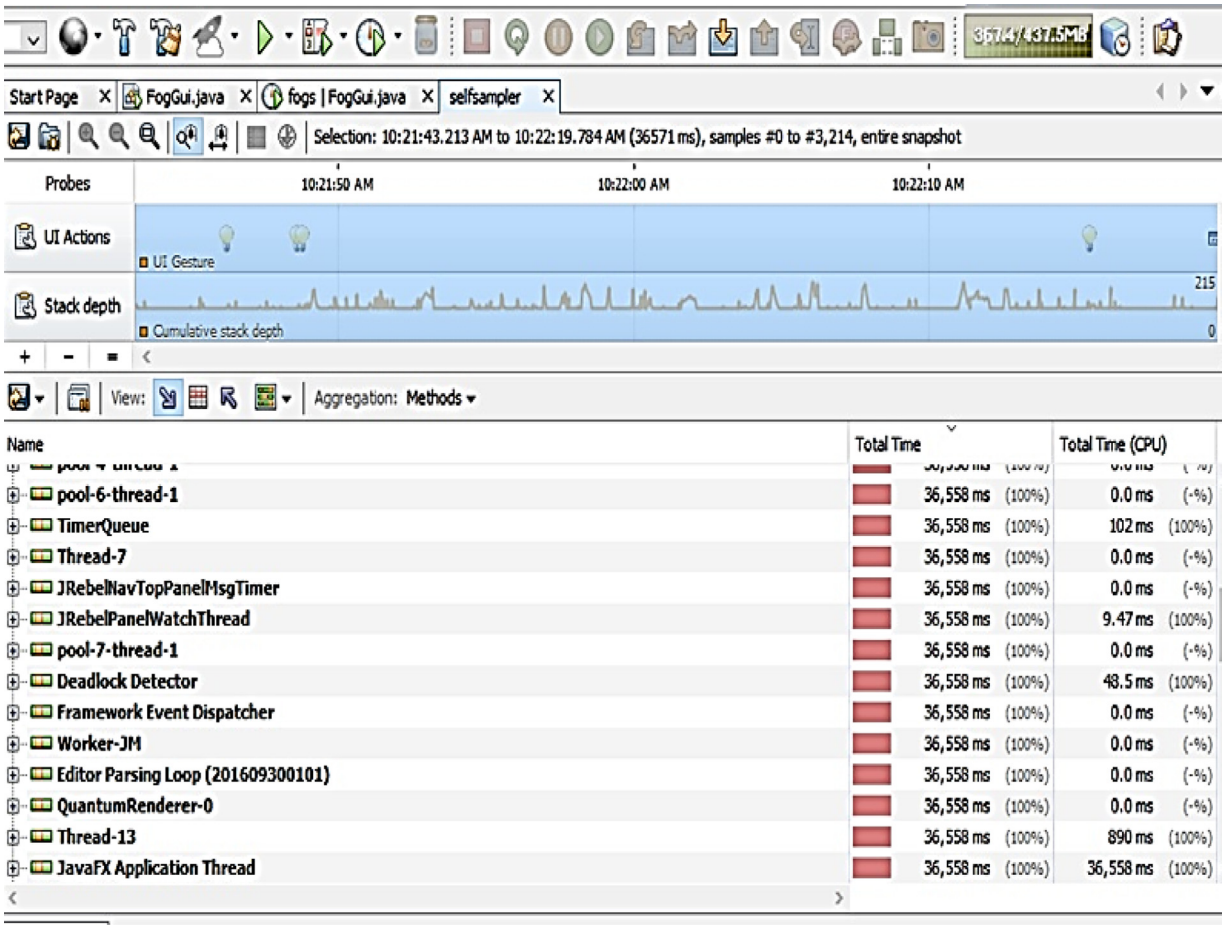

Fig. 15. The total time of execution for ongoing processes in fog nodes and cloud.

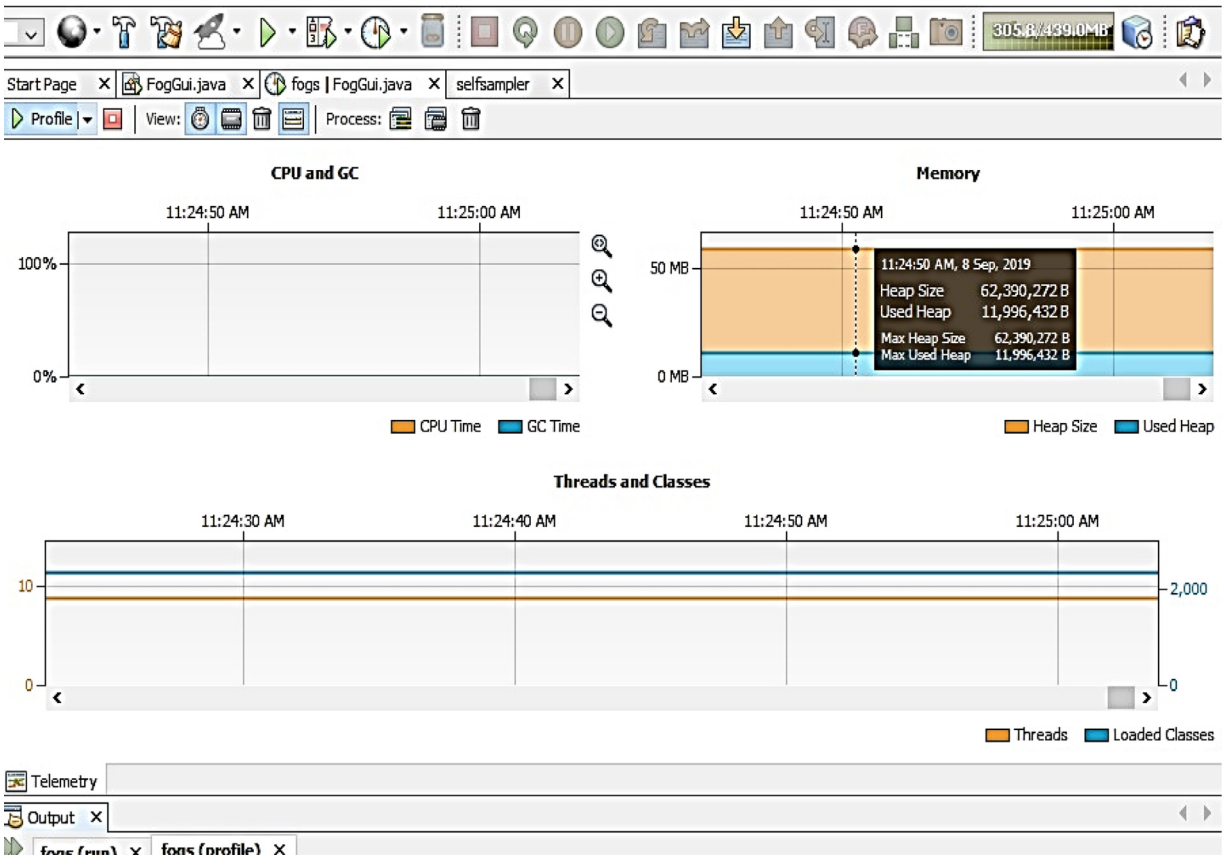

Fig. 16. The garbage collection (GC) and heap size in fog nodes

Table 5
Network links description for the configuration 1

Source	Destination	Latency(ms)
ECG_IoT1	Fog_device1	40
ECG_IoT2	Fog_device1	45
ECG_IoT3	Fog_device1	45
Fog_device1	Cloud_server1	70

Table 6
Network links description for the configuration 2

Source	Destination	Latency(ms)
ECG_IoT1	Fog_device1	40
ECG_IoT2	Fog_device1	45
ECG_IoT3	Fog_device2	50
ECG_IoT4	Fog_device2	50
Fog_device1	Master_Fog_Controller	55
Fog_device2	Master_Fog_Controller	60
Master_Fog_Controller	Cloud_server1	70

Tables 2–9 show the descriptions of the various devices and network link for the GUI in Figures 10-14. The data size for the PHD was defined in terms of megabytes (MB).

Figure 17 shows the throughput for FC nodes and cloud servers in Megabits per second (Mbps) for different physical topology configurations. The figure shows the throughput values for FC nodes is much greater when compared to the cloud servers. The throughput here is calculated by measuring the success rate of data packet transmission from fog nodes to end-user. Similarly, throughput values are also measured from one cloud server to end-users over a period at different configurations. The throughput increases with an increase in the number of healthcare IoT devices from Config.1-Config.5.

Table 7
Network links description for the configuration 3

Source	Destination	Latency(ms)
ECG_IoT1	Fog_device1	40
ECG_IoT2	Fog_device1	45
ECG_IoT3	Fog_device1	45
ECG_IoT4	Fog_device2	50
ECG_IoT5	Fog_device2	50
Fog_device1	Master_Fog_Controller	55
Fog_device2	Master_Fog_Controller	60
Master_Fog_Controller	Cloud_server1	70

Table 8
Network links description for the configuration 4

Source	Destination	Latency(ms)
ECG_IoT1	Fog_device1	40
ECG_IoT2	Fog_device1	45
ECG_IoT3	Fog_device1	45
ECG_IoT4	Fog_device2	50
ECG_IoT5	Fog_device2	50
ECG_IoT6	Fog_device2	50
Fog_device1	Master_Fog_Controller	55
Fog_device2	Master_Fog_Controller	60
Master_Fog_Controller	Cloud_server1	70

Table 9
Network links description for the configuration 5

Source	Destination	Latency(ms)
ECG_IoT1	Fog_device1	40
ECG_IoT2	Fog_device1	45
ECG_IoT3	Fog_device1	45
ECG_IoT4	Fog_device2	50
ECG_IoT5	Fog_device2	50
ECG_IoT6	Fog_device2	50
ECG_IoT7	Fog_device2	50
Fog_device1	Master_Fog_Controller	55
Fog_device2	Master_Fog_Controller	60
Master_Fog_Controller	Cloud_server1	70

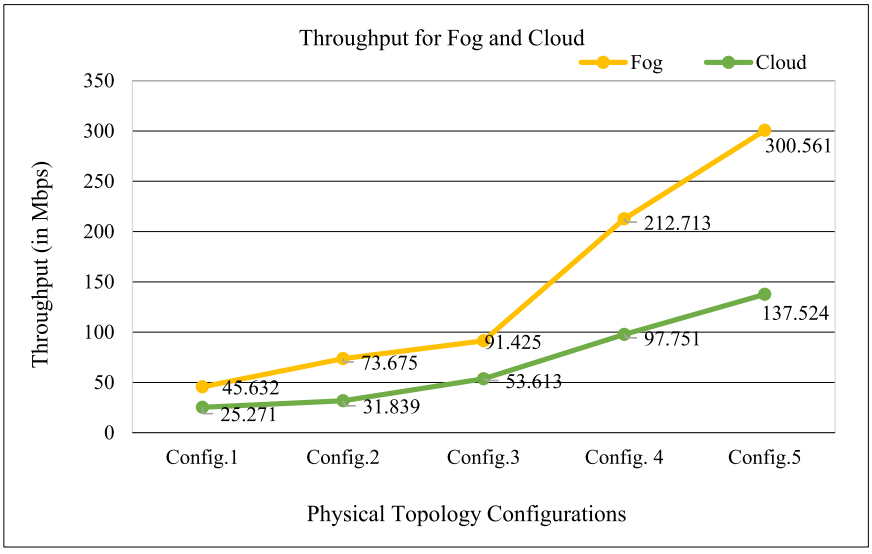

Fig. 17. Throughput for FC and cloud computing

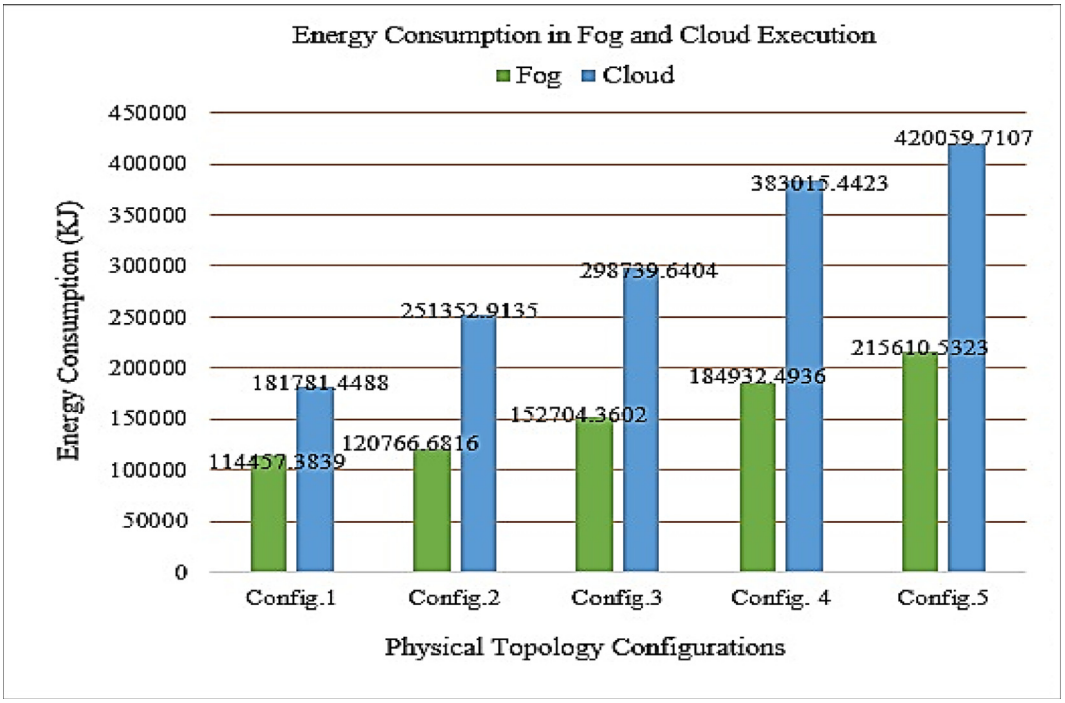

Fig. 18. Energy consumption (KJ) in FC and cloud computing

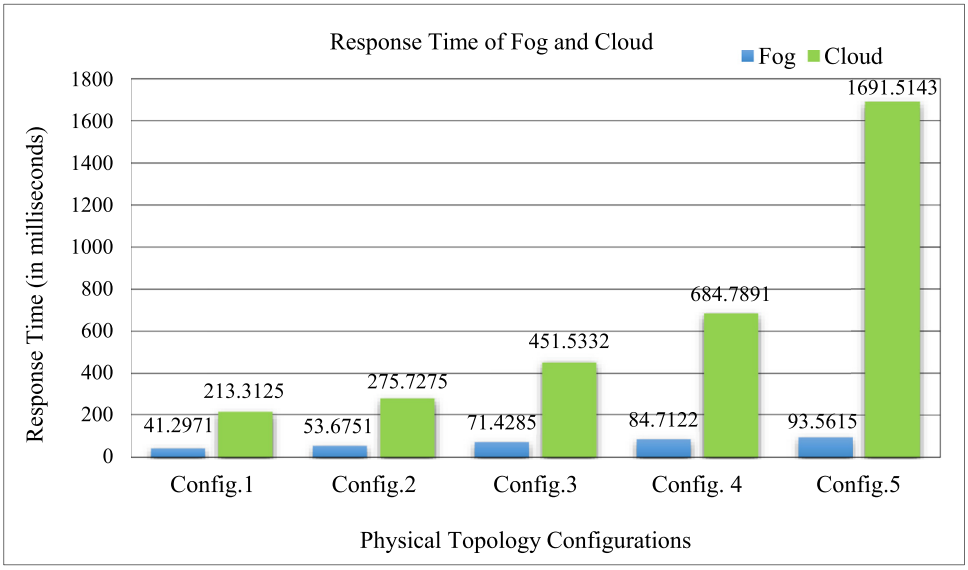

Fig. 19. Response time for FC and cloud computing

Figure 18 shows the energy consumption in FC and cloud execution for different physical topology configurations. By analyzing the figure, a conclusion can be drawn that the energy consumption in fog nodes is much lower than the energy consumption in cloud servers. The fast and excessive switching of processor speed due to a large amount of data generated by the healthcare IoT devices leads to inefficient utilization of data packet at the cloud and further increases the energy consumption. Here the high speed of processors in cloud servers causes larger values of energy consumption. The energy consumption increases with an increase in the number of healthcare IoT devices from Config.1-Config.5.

Figure 19 shows the response time of FC and cloud servers in milliseconds (ms) for different physical topology configurations. The figure shows the response time of fog nodes is much lesser when compared to the cloud. The response time increases with an increase in the number of IoT devices from Conflg.1-Config.5. The IoT devices in the Config.1, Config.2,

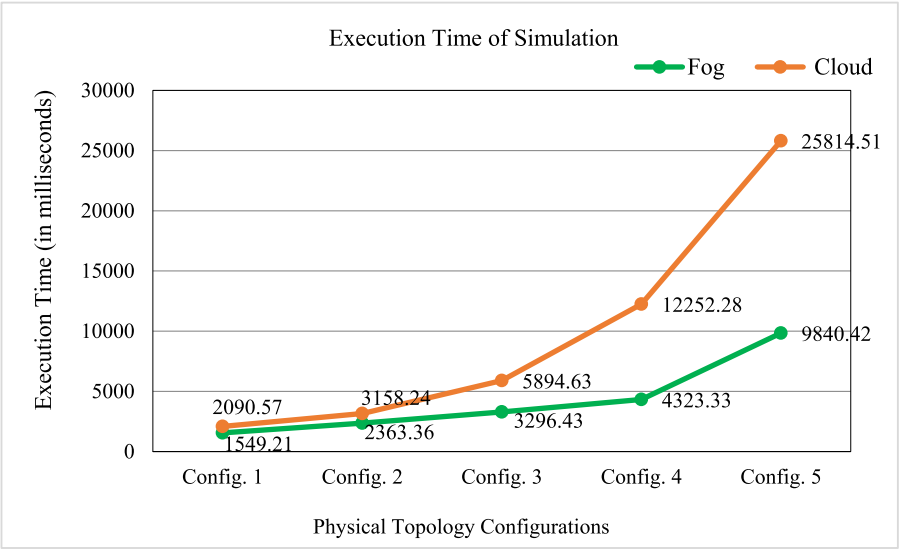

Fig. 20. Execution time of simulation comparison between FC and cloud

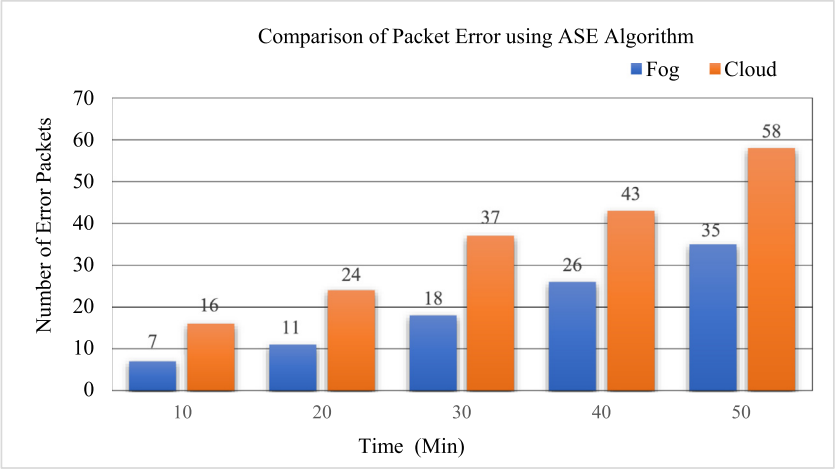

Fig. 21. Comparison of packet error

Config.3, Config.4, and Config.5 are increased from 3-7. The response time is calculated by considering the total amount of time taken by a fog node and cloud server to respond to a request for service by end-users or IoT devices. While calculating the response time, the transmission time for a moment can be ignored, the response time is the sum of service time and wait time. The wait time is the time spent by a data packet in the queue before being served.

Figure 20 shows the execution time of simulation comparison in milliseconds between fog nodes and cloud servers in different physical topology configurations. The figure shows the execution time for fog nodes is much lesser when compared to the cloud. The execution time of simulation increases with an increase in the number of IoT devices from Conflg.1-Config.5. The IoT devices in the Config.1, Config.2, Config.3, Config.4, and Config.5 are increased from 3-7

Software and simulator like SimBlock and iFogSim are used for verification of healthcare IoTs. We have designed five different configurations set up in the iFogSim simulator to check the number of PHD successfully sent to patients and doctors after authentication and verification.

Figure 21 shows the comparisons of packet error using the ASE algorithm between fog nodes and cloud servers at different time intervals. The figure shows the packet error in fog nodes is much lesser when compared to the cloud. The simulation of the ASE algorithm is conducted in iFogSim to record the number of packet error during real-time data transmission between healthcare IoT, FC nodes, end-users, and cloud servers.

The minimum number of packet errors in fog and cloud are 7 and 16. Whereas, the maximum packet error in fog and cloud are 35 and 58. The obtained results indicated the better performance of the proposed ASE algorithm in the

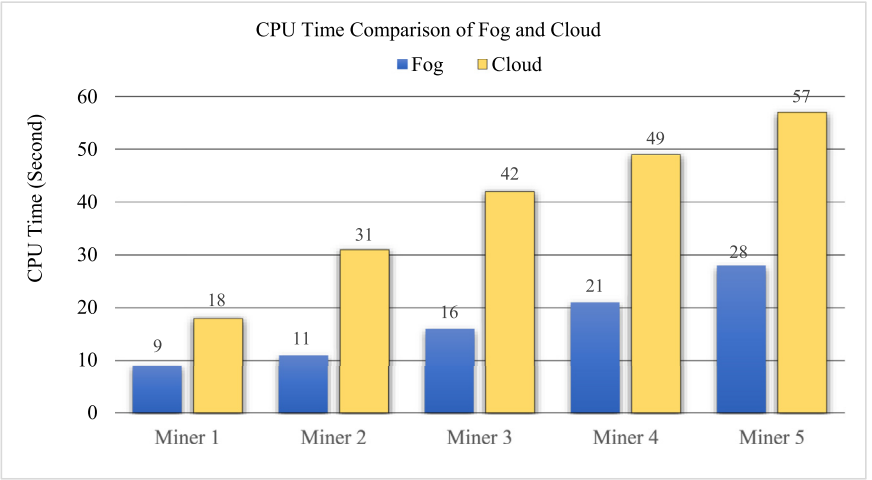

Fig. 22. CPU time comparison of Fog-PoW and Cloud-PoW

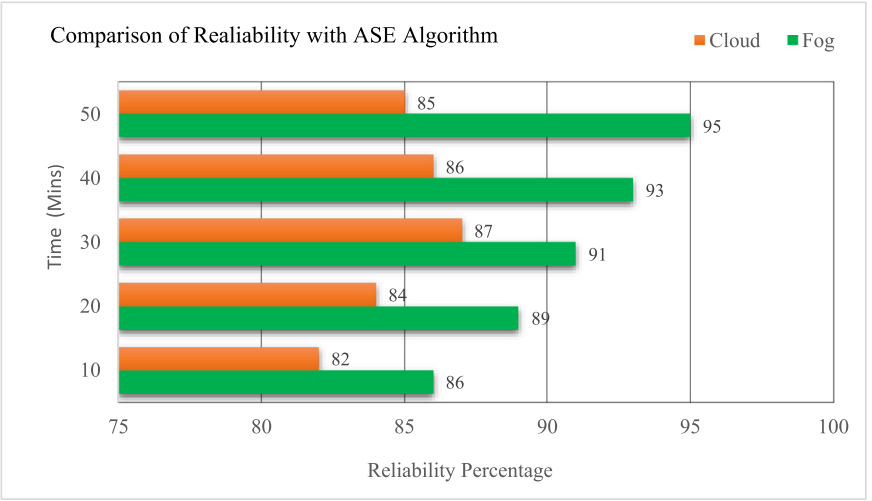

Fig. 23. Comparison of reliability in Fog-ASE and Cloud-ASE

FC environment. The algorithm for packet error comparison is tested on five different physical topology configurations at different time intervals. The packet error for the ASE algorithm increases with an increase in time.

Figure 22 shows the CPU time comparison of fog-PoW and cloud-PoW using the ASE algorithm in different miners. The figure shows the CPU time consumption in fog nodes is much lesser when compared to the cloud. The minimum values of CPU time for PoW in FC and cloud using iFogSim simulator are 9 seconds and 18 seconds at Miner 1. Whereas the maximum values of CPU time for PoW in FC and cloud environment are 28 seconds and 57 seconds at Miner 5. The obtained results indicated the better CPU performance of the proposed ASE algorithm in the FC environment. The algorithm for CPU time comparison is tested on five different physical topology configurations at different miners.

Figure 23 shows the comparison of reliability in fog-ASE and cloud-ASE at different time intervals. The figure shows the comparison of reliability in fog nodes is much greater when compared to the cloud. The classified ECG healthcare data is taken as an input value to the proposed system [44, 45]. The minimum percentage values of the ASE algorithm for reliability in FC and cloud using iFogSim simulator are 86% and 82%. Whereas the maximum percentage values of the ASE algorithm for reliability in FC and cloud environment are 95% and 87%.

The obtained reliability results indicated the better performance of the proposed ASE algorithm in the FC environment. The algorithm for reliability percentage is tested on five different physical topology configurations at different time intervals in minutes.

Figure 24 shows the number of blocks processed in fog and cloud along with the time required to process the blocks. The figure shows that the processing time for blocks in fog nodes is much lesser when compared to the cloud. The minimum processing time of the ASE algorithm for healthcare IoT in FC and cloud using the iFogSim simulator is 223 milliseconds

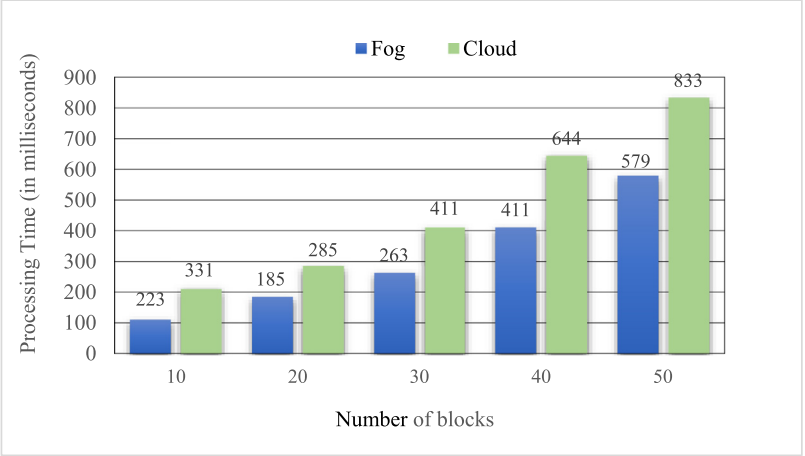

Fig. 24. Number of blocks in fog and cloud vs processing time

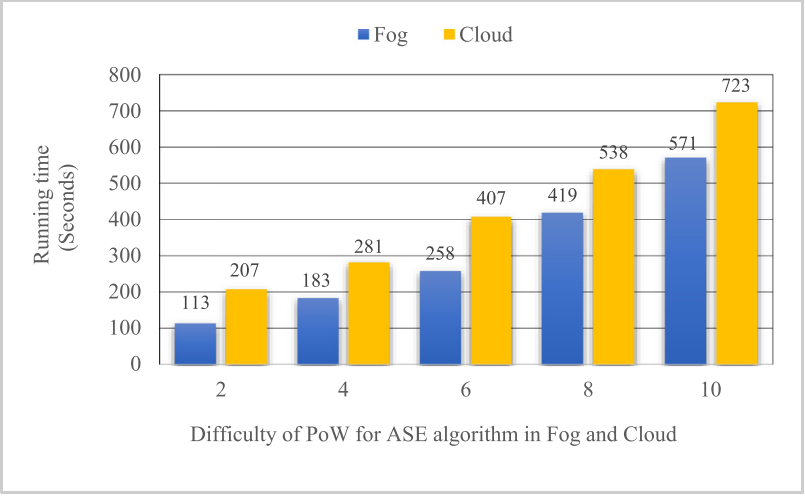

Fig. 25. Running time of ASE algorithm for PoW with the difficulty level

and 331 milliseconds with 10 blocks. Whereas the maximum processing time of the ASE algorithm for healthcare IoT in FC and cloud environment is 579 milliseconds and 833 milliseconds with 50 blocks. The obtained results for processing time indicated the better performance of the proposed ASE algorithm in the FC environment. The processing time of the ASE algorithm increases with an increase in the number of blocks.

Figure 25 shows the running time of the ASE algorithm for Proof-of-Work (PoW) with varying difficulty level in fog and cloud. The figure shows that the difficulty level in fog nodes is much lesser when compared to the cloud. The minimum running time of the ASE algorithm for PoW with difficulty level 2 in FC and cloud using the iFogSim simulator is 113 seconds and 207 seconds. Whereas the maximum running time of the ASE algorithm for PoW with difficulty level 10 in FC and cloud environment is 571 seconds and 723 seconds. The running time of the algorithm for PoW is tested on five different physical topology configurations at different difficulty levels. The running time of the ASE algorithm increases with an increase in the difficulty levels.

Figure 26 shows the malicious node percentage in fog and cloud along with the detection accuracy in percentage. The figure shows that the detection accuracy in fog nodes is much greater when compared to the cloud. The minimum detection accuracy of the ASE algorithm for malicious node percentage 5 in FC and cloud using iFogSim simulator is 61% and 59%. Whereas the maximum detection accuracy of the ASE algorithm for malicious node percentage 25 in FC and cloud environment is 91% and 83%. The ASE algorithm for detection accuracy percentage is tested on five different physical topology configurations at different malicious node percentage. The detection accuracy increases with an increase in malicious node percentage.

Figure 27 shows the comparison of reliability percentage for performance evaluation of the proposed ASE algorithm with the other existing state-of-the-art techniques such as FogBus, Femto cloud, BFAN, and BeeKeeper. Different existing algo-

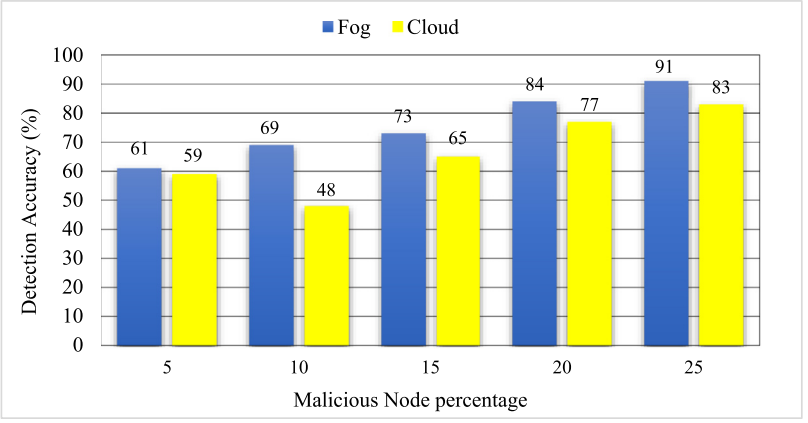

Fig. 26. Malicious node percentage vs detection accuracy

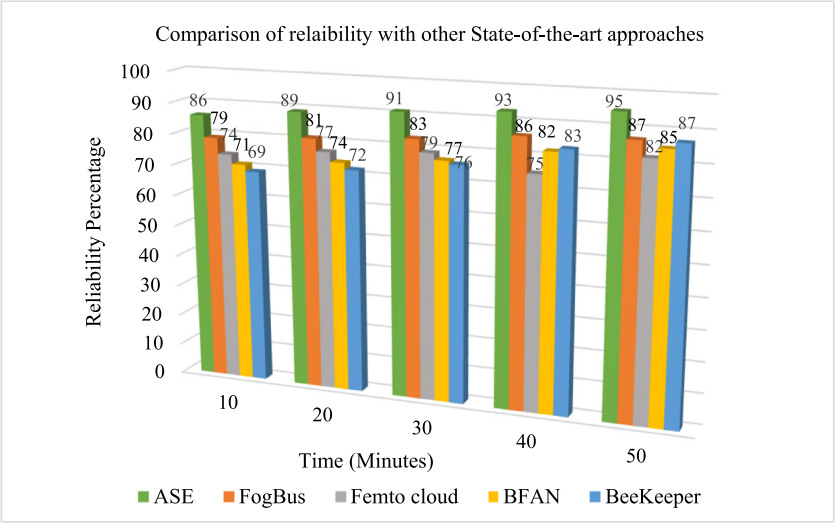

Fig. 27. Comparison of reliability for performance evaluation

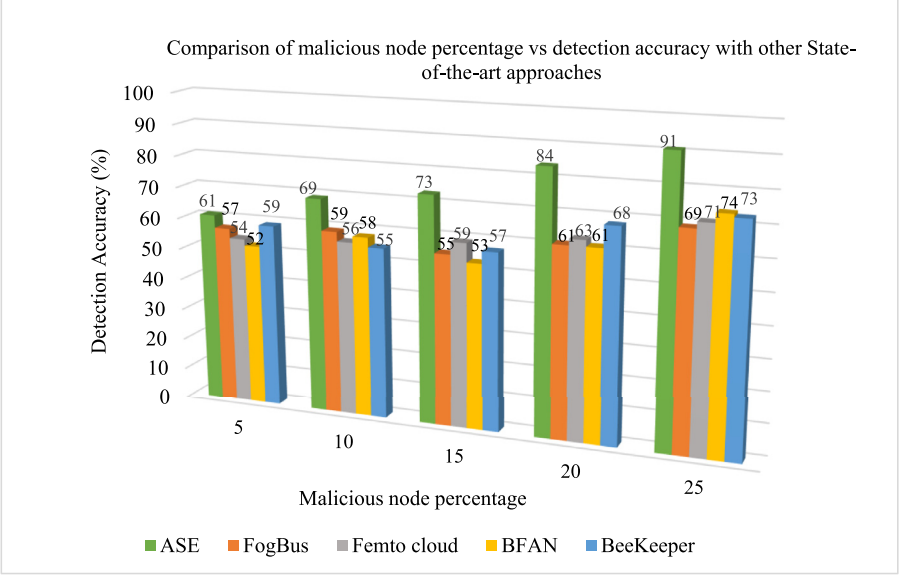

Fig. 28. Malicious node percentage vs detection accuracy performance evaluation

rithms are considered for benchmarking using the iFogSim simulator in five different physical topology configurations. The minimum reliability percentage is 69% for BeeKeeper. Whereas the minimum reliability percentage for the ASE algorithm is 86%. Similarly, the maximum reliability percentage is 87% for both FogBus and BeeKeeper. Whereas the maximum reliability percentage for the proposed ASE algorithm is 95%. The ASE algorithm easily outperforms the other techniques. The proposed algorithm yields marked improvement over the other techniques.

Figure 28 shows the comparison of malicious node percentage vs detection accuracy for performance evaluation of the proposed ASE algorithm with the other existing state-of-the-art techniques. Different existing algorithms are considered for benchmarking using the iFogSim simulator in five different physical topology configurations. The minimum detection accuracy is 52% for BFAN at malicious node percentage 5. Whereas the minimum detection accuracy for the ASE algorithm is 61% at malicious node percentage 5. Similarly, the maximum detection accuracy is 74% for BFAN at malicious node percentage 25. Whereas the maximum detection accuracy for the proposed ASE algorithm is 91% at malicious node percentage 25. The ASE algorithm easily outperforms the other techniques. From Figure 28 for the detection accuracy percentage, the proposed algorithm yields marked improvement over the other techniques.

13. Conclusion

The current trend of healthcare is mostly found in the digitization of data. Where smart contracts will play a major role. The IoT data need to be processed and monitored steadily. Healthcare IoT generates a large variety and veracity of PHD. Processing this amount of data leads to insecure transmission between IoT devices and users. Therefore, in this paper, we address the issue of healthcare IoT data authentication and IoT device identification. Next, we present a novel solution to process the PHD with improved security.

Traditional cloud servers work in a centralized manner to filter the PHD. These centralized servers are prone to a single point of failures. Moreover, healthcare IoT devices can be attacked by outside intruders, hackers, and malicious agents. This leads to the tampering of data. A large number of heterogeneous IoT devices leads to unreliable and unauthenticated PHD. Therefore, to overcome this above-mentioned problem we have proposed a three-tier FC-based blockchain architecture, a mathematical framework, an Advanced Signature-Based Encryption Algorithm (ASE), and an analytical model for healthcare IoT device identification and PHD authentication for secure healthcare IoT data transmission. The solution and implementation of the proposed work are conducted in iFogSim, SimBlock, and Python Editor tool.

The proposed algorithm improves the detection accuracy for malicious node along with reliability. Furthermore, the ASE algorithm reduces the packet error for PHD transmission between healthcare IoT and end-users. When compared for performance evaluation and analysis of results the proposed algorithm easily outperforms the existing state-of-the-art techniques and approaches such as Fog Bus, BeeKeeper, Femto cloud, and FBAN.

It has been established that the application of the proposed model and algorithm addresses a problem for PHD authentication and healthcare IoT device identification by minimizing the packet error and malicious node percentage. The proposed approach has a deeper impact on healthcare IoT and FC for throughput and execution time as the time-sensitive PHD can be transferred to patients and doctors in a single hop-count with minimum service delay. The processing of the healthcare data at the edge of IoT networks is secured in a decentralized manner using the blockchain technique. The future work includes testing the algorithm to reduce the complexity of the healthcare IoT-FC system with the increase in the number of IoT and fog devices. The proposed approach is also useful for telesurgery and Augmented Reality (AR). Moreover, the proposed technique in future can also be used for other IoT applications like onshore and offshore oil and gas monitoring. In future research, we will be testing the ASE algorithm to overcome the scalability limitation of blockchain when used with healthcare IoT and FC.

Declaration of Competing Interest

The authors indicate that they have no conflicts of interest.

Acknowledgement

This publication has emanated from research supported in part by a research grant from Cooperative Energy Trading System (CENTS) under Grant Number REI1633, and also by a research grant from Science Foundation Ireland (SFI) under Grant Number SFI 12/RC/2289_P2 (Insight), co-funded by the European Regional Development Fund.

References

[1] L. Bittencourt, et al., The internet of things, fog and cloud continuum: Integration and challenges, Internet of Things 3 (2018) 134–155.
[2] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, E. Hossain, A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes, IEEE Access 8 (2020) 118433–118471.
[3] S. Shukla, M.F. Hassan, M.K. Khan, L.T. Jung, A. Awang, An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment, PloS one 14 (11) (2019) e0224934.
[4] A. Waqar, A. Raza, H. Abbas, M.K. Khan, A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata, Journal of Network and Computer Applications 36 (1) (2013) 235–248.

[5] G. Srivastava, J. Crichigno, S. Dhar, A light and secure healthcare blockchain for iot medical devices, in: *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*„ IEEE, 2019, pp. 1–5.
[6] T.M. Fernández-Caramés, P. Fraga-Lamas, A Review on the Use of Blockchain for the Internet of Things, Ieee Access 6 (2018) 32979–33001.
[7] M. Tahir, M. Sardaraz, S. Muhammad, M. Saud Khan, A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics, Sustainability 12 (17) (2020) 6960.
[8] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey, IEEE Access 8 (2020) 16440–16455.
[9] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3680–3689.
[10] F. Jamil, S. Ahmad, N. Iqbal, D.-H. Kim, Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals, Sensors 20 (8) (2020) 2195.
[11] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: A block architecture, IEEE Access 6 (2018) 32700–32726.
[12] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and iot integration: A systematic survey, Sensors 18 (8) (2018) 2575.
[13] B.W. Nyamtiga, J.C.S. Sicato, S. Rathore, Y. Sung, J.H. Park, Blockchain-Based Secure Storage Management with Edge Computing for IoT, Electronics 8 (8) (2019) 828.
[14] A. Sonnino, M. Al-Bassam, S. Bano, S. Meiklejohn, and G. Danezis, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," *arXiv preprint arXiv:1802.07344*,2018.
[15] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, R. Lu, User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption, IEEE Transactions on Computers 65 (9) (2015) 2939–2946.
[16] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[17] S.K. Singh, S. Rathore, J.H. Park, Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence, Future Generation Computer Systems 110 (2020) 721–743.
[18] A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari, A. Romano, Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds, Sensors 20 (9) (2020) 2590.
[19] W. Wang, et al., A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.
[20] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, W. Liu, Blockchain trust model for malicious node detection in wireless sensor networks, IEEE Access 7 (2019) 38947–38956.
[21] L. Zhou, L. Wang, Y. Sun, P. Lv, Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation, IEEE Access 6 (2018) 43472–43488.
[22] L. Wu, X. Du, W. Wang, B. Lin, An out-of-band authentication scheme for internet of things using blockchain technology, in: 2018 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2018, pp. 769–773.
[23] A. Ouaddah, A.Abou Elkalam, A.A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT, in: *Europe and MENA cooperation advances in information and communication technologies:*, Springer, 2017, pp. 523–533.
[24] T. Alam, "IoT-Fog: A communication framework using blockchain in the internet of things," *arXiv preprint arXiv:1904.00226*,2019.
[25] K. Singh, O. Dib, C. Huyart, K. Toumi, A novel credential protocol for protecting personal attributes in blockchain, Computers & Electrical Engineering 83 (2020) 106586.
[26] B. Bhushan, A. Khamparia, K.M. Sagayam, S.K. Sharma, M.A. Ahad, N.C. Debnath, Blockchain for smart cities: A review of architectures, integration trends and future research directions, Sustainable Cities and Society 61 (2020) 102360.
[27] N. Islam, Y. Faheem, I.U. Din, M. Talha, M. Guizani, M. Khalil, A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services, Future Generation Computer Systems 100 (2019) 569–578.
[28] P. Singh, A. Nayyar, A. Kaur, U. Ghosh, Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities, Future Internet 12 (4) (2020) 61.
[29] M.H. Ziegler, M. Groβmann, U.R. Krieger, Integration of fog computing and blockchain technology using the plasma framework, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 120–123.
[30] L. Chen, Z. Wang, F. Li, Y. Guo, K. Geng, A Stackelberg Security Game for Adversarial Outbreak Detection in the Internet of Things, Sensors 20 (3) (2020) 804.
[31] L. Bittencourt, et al., The internet of things, fog and cloud continuum: Integration and challenges, Internet of Things (2018).
[32] M.G.R. Alam, Y.K. Tun, C.S. Hong, Multi-agent and reinforcement learning based code offloading in mobile fog, in: 2016 International Conference on Information Networking (ICOIN), IEEE, 2016, pp. 285–290.
[33] K. Sambyo, C.T. Bhunia, Application of Multi Level ATM in Reducing Latency in Clouds for Performance Improvement of Integrated Voice, Video and Data Services, in: 2014 11th International Conference on Information Technology: New Generations, IEEE, 2014, p. 607. -607.
[34] K. Habak, M. Ammar, K.A. Harras, E. Zegura, Femto clouds: Leveraging mobile devices to provide cloud service at the edge, in: 2015 IEEE 8th international conference on cloud computing, IEEE, 2015, pp. 9–16.
[35] S. Tuli, R. Mahmud, S. Tuli, R. Buyya, Fogbus: A blockchain-based lightweight framework for edge and fog computing, Journal of Systems and Software (2019).
[36] S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities, IEEE Access 5 (2017) 26521–26544.
[37] S. Tuli, et al., Healthfog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated iot and fog computing environments, Future Generation Computer Systems 104 (2020) 187–200.
[38] M. Wazid, A.K. Das, S. Shetty, M. Jo, A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things, IEEE Access 8 (2020) 88700–88716.
[39] V. Chamola, V. Hassija, V. Gupta, M. Guizani, A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact, IEEE Access 8 (2020) 90225–90265.
[40] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, K. Shudo, SimBlock: A blockchain network simulator, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2019, pp. 325–329.
[41] R. Banno, K. Shudo, Simulating a blockchain network with SimBlock, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 3–4.
[42] K. S. Awaisi, A. Abbas, S. U. Khan, R. Mahmud, and R. Buyya, "Simulating Fog Computing Applications using iFogSim Toolkit."
[43] H. Gupta, A. Vahid Dastjerdi, S.K. Ghosh, R. Buyya, iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments, Software: Practice and Experience 47 (9) (2017) 1275–1296.
[44] K. Balaskas, K. Siozios, ECG Analysis and Heartbeat Classification Based on Shallow Neural Networks, in: 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, 2019, pp. 1–4.
[45] T.N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, H. Tenhunen, Fog computing in healthcare internet of things: A case study on ecg feature extraction, in: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, IEEE, 2015, pp. 356–363.