INTEGRATION OF BLOCKCHAIN TECHNOLOGIES INTO IoT SECURITY

Deepankar

Project report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

in Partial Fulfillment of the

Requirements for the

Final Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

December 2020

INTEGRATION OF BLOCKCHAIN TECHNOLOGIES INTO IoT SECURITY

Deepankar

Approved:

Sergey Butakov [Original Approval on File]

Sergey Butakov Date: December 10, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: December 15, 2020

Dean, Faculty of Graduate Studies

Integration of blockchain technologies into IoT security

Deepankar (139984)

dlnu3@student.concordia.ab.ca

Research Advisor: Dr. Sergey Butakov

sergey.butakov@concordia.ab.ca

Department of Information Systems Security Management

Concordia University of Edmonton, Edmonton, Alberta T5B 4E4 Canada

ABSTRACT

The role of wearable connected devices in healthcare is rapidly gaining importance. Collection of data through these smart devices is a key instrument in advancing biomedical research and in tracking of health indicators of an individual. Highly sensitive medical data requires advanced protection mechanisms to maintain data privacy and validation in a resource-efficient manner to protect it from forgery or unauthorized use. Blockchain is one of those technologies that can be used in various forms to improve data privacy. The proposed research suggests a way to implement blockchain in an ecosystem of medical IoT devices to achieve non-repudiation and better protection of collected data. The architecture assumes that all push and pull operations on IoT data are being logged into two blockchains – public and private. The arrangement allows to have protected track of data enquiries and updates to achieve user confidence and non-repudiation.

I INTRODUCTION

Wearable gadgets are one of the emerging technologies aimed at the continuous recording of real-life physical activities, behavior and daily routine of an individual. The data which is commonly recorded consists of vital signs such as heart rate, body temperature, blood pressure, oxygen saturation, electrocardiogram (ECG), ballistocardiogram et cetera. Wearables and Medical IoT Interoperability & Intelligence (WAMIII) supported by the Internet of Medical Things (IoMT) is a growing field [1]. The demand to improve WAMIII devices for healthcare purposes is increasing in market. In most of the cases, a smart device such as a mobile phone is used to collect information and transmit it to a remote server for analysis of data and storing it in a presumed secure place. There are mainly two types of smart wearable devices which are used in healthcare. First, specialized devices, that are solely for medical purposes, used to monitor walking patterns, including the accelerometer, multi-angle video recorders, gyroscopes etc. Others are consumer devices developed for health-conscious clients. They are represented in market mostly as on-wrist trackers such as Fitbit and iWatch [1].

Moving further, these wearables or IoMT devices have a basic three-layer structure which consists of perception, network and application [2]. The perception layer is used to collect or record data from an individual or surrounding environment through various devices. The network layer is used to transfer the data collected by perception layer for further analysis. The transfer of data can be wired or wireless. The application layer helps to analyse data which is then further used to offer medical facilities and fulfill the final individual needs. The security of data collected, and its privacy are a major concern in the IoMT process. The individual data stored and sent should be secured. More security can be added or developed according to the usage requirements. Wearable IoMT devices facilitate improved personal health monitoring but they also create pressure on data security and privacy protection. The healthcare data is a lucrative target and there is always a demand to secure it. Furthermore, there is a strong need to maintain accurate timeline of events, log information of actions and integrity of data. Blockchain can be used to record the events from its origin to the current state and act as a detective control whenever there is a unauthorized access of data[3].It can provide a mechanism to notify the user when there is any privacy breach and help to implement non-repudiation. This paper suggests practical ways on how the blockchain can be embedded into IoT ecosystem to address the above-mentioned problems.

The paper has been organized as follows: Section I provides a basic introduction to the research topic. Section II looks at the related works in this area.

Section III discusses the proposed approach on blockchain use in the ecosystems of medical IoT devices; Section IV discusses potential attacks that can happen in the ecosystem and Section V outlines the conclusion.

II RELATED WORKS

The number of IoT wearables is growing exponentially in market. These are manufactured according to the rising demands and needs of the consumers and industry. Wearables act as lifestyle devices, where majority of people perceive fitness as a lifestyle rather than just an activity [1]. In addition to this wearable technology, applications are developed for prevention of various diseases, and maintenance and tracking of health such as weight control, psychological behavior, and physical activities[1]. These devices can improve some of the clinical decisions. These devices are very popular among old age patients for managing their health and rehabilitation outside of hospitals[3]. Some of the devices are:

- Fitness Tracker
- Wearable ECG / Blood Pressure Monitors
- Smart / Sport watches
- Implantable IoT devices such as infusion pumps, pacemakers, etc.
- Military wearable sensors
- Skin patches
- Biosensors - Biosensors are the upcoming wearable medical devices that are different from wrist trackers and smartwatches [1]. These are developed to react only with a particular substance and the result of this reaction comes in the form of messages that can be analyzed by a microprocessor.

Wearable devices are functioned to perform their specific task so that the required information regarding user can be collected, transmitted, and analyzed. The next section discusses about the basic process of collecting data in traditional healthcare network.

2.1 Basic process of collecting data on an IoT based Healthcare Network

The wearable technology usually works by connecting to a smart device such as a mobile phone. The benefit of using mobile device is that the data can be stored and communicated securely. The consumer wearables such as lifestyle wearables do continuous reading of data and information which is collected and maybe needed for further analysis. Some firms use cloud computing for the storage of data which may have live encryption policy and here storage may not be a big concern[4]. However, ethical issues regarding the usage of stored data at cloud by different firms may be of concern. Tech giants can use this information to track the behavior of user and can develop or modify their products according to user liking. If the wearable device has cellular connectivity, then the data can be sent directly to the cloud storage [4]. The informative stored data which is on user phone, cloud storage or desktop, can be used by medical practitioners, firms or by the user itself depending upon the need of an individual. This type of process is very useful for a sports person. The wearable device which they use can help them to track their activity and performance. In addition to this, users can also monitor their sleeping cycle. Using this technology helps to store data and access it at anytime and anywhere through internet. Sportspersons can also share this data with their coach or medical adviser to have a check on their performance and health.

Body Sensor Network (BSN) is another term of technology used in IoT based modern health care system [3]. In BSN a number of sensors are placed on the body and surroundings of the patient to monitor the user's activity. These sensors are connected to a local processing unit – usually the smart phone – which, in turn, further sends data to a physician or a medical team through various communication channels. The ecosystem is presented in Figure 1.

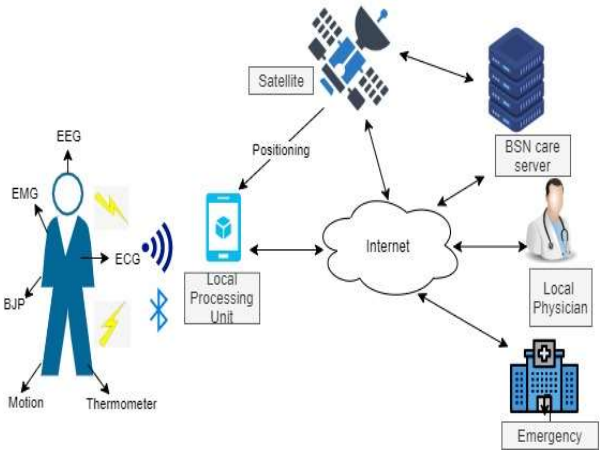

Fig 1. BSN IoT-based modern Healthcare System. Adopted from [3]

BSN model consists of two types of sensors known as in-body and on-body sensor network[3]. In-body sensor network helps in communication of implanted devices to send data to the medical team server, and on-body sensors such as wearables devices send data to the server through various channels. Figure 1 shows the basic framework of BSN based healthcare system. In Figure 1, there are several areas where threats can

appear in the BSN network, such as at the user side, at the processing unit, between transmission of data and untrustworthy medical personnell.

2.2 Security issues related to IoT devices

Security of data is one of the key concerns of people and of any organization system. Different people see security in different context. In general, security of data means confidentiality, integrity, accountability of the entire collected, communicated and stored data for the organization system and for the individual himself. In this digital world, whole communication of data in sensor network is wireless. This can raise many security issues. Some of the security challenges related to wearables and BSN based IoT devices are:

A. Data Confidentiality

Data privacy is now a days a major concern for people. It is very important to protect personal data from disclosure. In health care sector, data collected using wearable and other IoT devices should comply with the HIPAA regulations [2].The data should not get breached to an external network. In IoT devices, most of the communication is through wireless, and sensitive data is forwarded to other devices or systems. An attacker can eavesdrop on the communication and can collect the essential data of the users and patients [2]. This type of attack can cause great damage to the user and organization because attacker can use this information for illegal purposes and for defaming the organization. To mitigate these types of attacks, an adequate cryptographic scheme should be followed. Keys are the main component of cryptography. There should be a secure key agreement for sharing and distribution in sensor nodes [2]. Encryption of data plays an important role in authenticating the data and prevents any one from gaining privilege to personal information.

B. Integrity of Data

The lack of integrity of data can cause a major problem in healthcare environment. The IoT devices mostly communicate wirelessly, therefore an attacker can add some bits or fragments in the communicating data. This will change the meaning of the data received at end user side. This type of attack is very dangerous when there is emergency and whole patient data is changed [3]. Loss of integrity of data can also occur due to lose connection in various IoT devices communication nodes.

C. Authentication of Data Sent

The communication of data is wireless in an IoT based healthcare system. All data of the user is sent to the end user coordinator by various sensor nodes. In response to collected data, the coordinator sends a reply. In this scenario, authentication plays an important role. Authentication helps in identifying the users at each end [3].

D. Anonymity

The anonymity helps in hiding the source of packets during a wireless communication [3]. It ensures that attacker can neither tell or identify the patient and neither he or she can tell whether two conversations originated from the same patient or not. This increases the confidentiality of the service [3].

As a result of concerns related to all of the above issues, Food and Drug Administration (FDA) has issued multiple alerts to the companies and people about various vulnerabilities that have been found in IoT healthcare devices. In response to recalls, the manufactures had to call back devices from market because of the serious danger it could have caused to people. One of the examples of device recalls were Medtronic's MiniMed insulin pumps that were taken off the market due to potential cybersecurity risks. FDA has recommended that the patients using these models should switch their insulin pumps to models that are "better equipped to protect against potential risks" [5]. The discovered vulnerability potentially allowed the third party to collect vital information of a patient and to connect to device and change settings on insulin pump.

Considerations provided above make a strong call for the need to address the security and privacy issues in medical IoT ecosystems. Blockchain technology can be used as one of the tools to achieve better data protection. The blockchain-based approaches can address some of the issues mentioned above. Blockchain technology can help to achieve better security by adding enhanced privacy, full traceability of transactions, accurate timestamping etc. The integration of blockchain technology and IoT can provide a large potential in providing better security services in the field of healthcare system. Blockchain can enrich the IoT by providing a trusted share network where information is traceable. It can provide better security through enhanced privacy, better protection of transactions, full traceability, accurate timestamping which other technologies still struggle to provide to full extent.

2.3 Blockchain

Blockchain technology is seen as one of the emerging technologies which can play a constructive role in controlling, managing, and securing the IoT devices. Blockchain can be a potential technology to provide a reliable and enhanced security solution as

compared to the existing ones. This section provides a brief description about the blockchain and how it can play a major role in securing IoT devices.

The concept of blockchain was first given and described in Satoshi's paper for the Bitcoin payment system [6]. The author defines blockchain as a distributed ledger based on the cryptographic protocols. The paper explains how blockchain is resistant to tampering, is driven to network consensus and how data can be sent and stored in a peer-to-peer approach. In paper [7], the authors discuss the use of off-chain storage systems with blockchain to keep collected health care data and transactions secure. The data collected in healthcare is much larger than the data collected in Bitcoin or in public blockchains. Therefore, use of off-chain storage will be viable solution to store such a large size healthcare data.

In [8] the authors introduced a method of using blockchain to facilitate secure communication to end-points of the clinical trials. Irving and Holden have confirmed the usage of blockchain as a low cost, secured and verifiable method to audit. They also show how different aspects of security can be achieved by using blockchain network in IoT based network. Fujimura et al [9], in his paper, explained a method for the protection of new video content by giving the owner the control to access levels required by a license to use video. The proposed method uses the adjustment of an average interval time in which a new block is created from an old block. The author was able to adjust time from ten minutes to five seconds for the creation of new block in his method [9]. In paper [10], the author discusses about how a blockchain technology can be used to make the network tamperproof in healthcare. It also discusses about the benefits of using blockchain in healthcare.

It is said that the blockchain technology is seen as a secure technology because of its tamper evident and tamper resistant design but it is not exactly true. According to NISTIR 8202, the transactions that have not yet been published in the block within the blockchain are vulnerable to some attack. In addition to this, the newly coded application mainly using smart contracts may contain some vulnerabilities which can be discovered and exploited by attackers and can launch zero-day attack [11]. In the paper "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", the researchers have explained that how the smart contracts in blockchain technologies can be used to trigger alerts for the patients and the healthcare providers at every access point to data. They also added how the blockchain can solve current problems of poorly managed data [12].

The proposed research depicts problems in the healthcare sector using IoT devices as wearables to collect vital information of the people and how the integration of blockchain can help in solving those problem in a secure manner. Several healthcare blockchain implementations have been reviewed in terms of realization of their benefits and limitations. By studying the related work, a blockchain design has been proposed which can overcome many security issues such as non-redundancy, confidentiality, integrity, and availability of data. The model will act as a detective control whenever there is a unauthorized access of data. It provides the mechanism to notify the user when there is any privacy breach. The proposed research would contribute to studies on the blockchain technology and its implementation with IoT devices in healthcare environment. This approach can be used by the healthcare industry to implement non-repudiation and authentication detection scheme making the network secure and detective.

III PROPOSED APPROACH

3.1 System Design

The proposed IoT+blockchain ecosystem consists of the following components:

a. Client and IoT device

This component represents a user/patient and IoT device that she or he uses. In health care system there are sensors which collect vital information of a patient on real-time basis. The sensors on a device will act as nodes to collect patient data in the proposed ecosystem.

b. Processing Unit

The main node will be the processing unit such as smartphone or computer which will act as a gateway to the blockchain and collect information in encrypted form. There is different form of processing unit at client and hospital sides. This device will be responsible to add critical information to blockchain. Examples of such information may include patient id, digital signature, hash of collected data and other information as needed.

c. Hospital Management

The hospital management contains all the medical departments/doctors of the hospital who are authorized to work with patient data. They will have access to the application (-s) connected to the healthcare public blockchain described next.

d. Healthcare public blockchain

The healthcare public blockchain is publicly accessible to all the healthcare ecosystem members, but not to any third person out of the system. The healthcare public blockchain will be controlled and maintained by the local healthcare authority. This blockchain contains the transaction data such as digital signatures of user, an event the ecosystem participant tries to perform, patient ID, new data or updated data, timestamp and information of the member who tries to access the data.

e. Private healthcare blockchain

Every patient has its own private blockchain in proposed ecosystem and she/he can exercise full control on it. The patient private blockchain will be in custody of the local healthcare authority and will be stored on secured cloud network. The backup of it will be stored on a remote secured cloud depository and will be accessible in any case of crisis to restore all data. The patient will have all the rights on its private blockchain, including right to be forgotten so that the private blockchain can be permanently removed on her/his request. This private blockchain consists of transaction data such as digital signature of patient, its unique patient ID, hash of the data saved in data repository and access log which contains information that who can access data and timestamp. It also maintains the log of when user gave or revoke the access.

f. Data Storage

It is the storage point which contains all the patient's medical information. It can exist in a form of a conventional database which supports blockchain technology. Interplanetary File System (IPFS) cloud-based storage system can be used in this role as it has proper integration with blockchain [13].

g. Smart Contract Platform

An open platform is needed to write and implement complex operations on the blockchain. One of the examples of such platforms could be Ethereum which enables developers to build and deploy de-centralized applications. Ethereum allows user to configure smart contracts by using scripting language to a wider range of tasks. Smart contracts are basically scripts or codes that are implemented on blockchain, wait for the condition to get validated and act accordingly [12]. Smart contract on each private and public blockchain will act as a programmed function to define access control, data index / pointer in the cloud storage, retrieval of data and check if the file hash matches the payload to cloud storage. Smart contract execution will also add time and digital signature of the patient to the blockchain whenever data items are being collected.

The proposed approach aims at using two blockchains for maintenance of records within the activities performed by the user/patient, data server, and the third party / the health service provider. The private block chain is used to define an access grant by the client and to save the essential data in cloud. By having the access grant control, the third party will not be able to access any kind of information from the system, this provides user privacy to some degree. It also fetch and maintains a log information regarding, who tries to access the data and for what purpose, with a timestamp, whenever there is request from the public blockchain for enquiry to access data in the cloud. Whereas, the public block chain is used to record access data from cloud by the healthcare / third party. It maintains a log information about the access requests and actions performed by the healthcare or by any other third party. Public blockchain also contain information regarding the fact that at what time user grant or revoke the access to the data. This will help to avoid user to deny the fact that he/she provided or revoked the access. The whole system assures alerting the IoT device owner or data owner when there is an access to the private data area. Also, it establishes non-repudiation mechanism, which will not allow the third party to deny the fact that they accessed the data. The approach is explained with the help of a time graph which represents the system design attributes on the top and events occurring as time goes down on the data flow in figure 2.

3.2 Data Flow in the Proposed System

a) Sensor Data Collection

The overall procedure is to collect sensor data on the producer side by the main processing unit from sensor, digitally sign the data and encrypt the generated payload. The collected data is then saved to cloud depository and resulting hash is stored in Ethereum block chain. The patient data will be created and stored in patient private folder on the processing unit with various fields which will be assumed to be collected from the sensor. In the client private blockchain, sensors and the local processing unit (Figure 1) act as nodes. To begin**,** every device must authenticate itself using private and public key. These keys are specific to each sensor. The processing unit will store all the keys in its local storage to recognize

authenticated nodes faster. This activity is represented by query (1) on the timing diagram - Figure 2.

b) Client connection to blockchain

After device registration, a new block is created which will have data collected by IoT devices and connection is established with processing unit. This block will then be added to the private blockchain using processing unit which will act as a patient private block (2). This patient private block will have its own local memory which will have information such as digital signature, hash of data collected, index number where the data is stored, patient unique id, access details given by the client and other information.

c) Store Collected Data in the Cloud Depository

Only the critical data is being stored in the IPFS cloud interface (3). When data is stored in the cloud, the index number of stored data is fetched (4) by the private blockchain and an alert message will be sent to patient if there is failure of data storage in the IPFS (5). The mere example of store data is shown in table 1.

Serial No.	Payload Item	Brief Explanation	Example Data
1	Patient id	Unique id of patient	26
2	Patient name	Name of the patient	BOB
3	Digital signature	Digital signature of the patient	####
4	Heartbeat	Units of Heartbeat (BPM)	72
5	Time stamp	Time at which data collected	2020-04-15 22:10:20
6	Sensor type	Type of sensor used	DHT 11
7	Device ID	IoT device ID	HB sensor
8	Device IP	IP of IoT device	192.168.0.18

Table 1. Example of stored data in IPFS

d) Hospital Management sends request to access Data from the Storage

A nurse or a doctor who has access to the public blockchain of healthcare will generate a request using their login credentials through application to access the stored data of the patient (6). The smart contract at the public chain will contain programmable function which will collect data such as member id, digital signature, timestamp, event to perform and the type of access it wants to collect log information. This log information will be added to public blockchain with information, such as, who requested what type of event at what time (7).

e) Checking for Access or Permission Level

The public block chain triggers a communication with patient private blockchain with the help of its unique ID and looks if the access is granted to hospital employee (8). Once permission is granted, the system is available to interact with the private chain of patients and cloud data repository.

f) Adding Event Information to Private Block of the Patient

A new block will be added to the private block chain containing log information regarding who has requested the grant and what type of activity is requested at what time (9). The event information collected by smart contract at public block chain will be added to the patient private block chain.

g) Members Access the Data

If an access is granted, the index number of the saved information in data repository will be fetched from the private block chain else the access will be denied (10) plus the log information of public blockchain will be updated regarding when user gave and revoke access. The fetched index number will be used by the public blockchain to access data from the cloud (11). If access is allowed to logged person and there is any modification done in data, then an alert will be sent to the client (12). In addition to this, the patient will have full control over his private blockchain as the permission privileges will be added by the patient himself. When anyone wants to access data or request to access data, first a alert will be sent to the patient and a log will be added to patient private blockchain to keep track.

Digital signature provides authentication of data in the above approach whereas access rules or privileges added by the patient on his private block chain define accessibility to data and its privacy. Hash of the data can be used to check the integrity of data stored in cloud system.

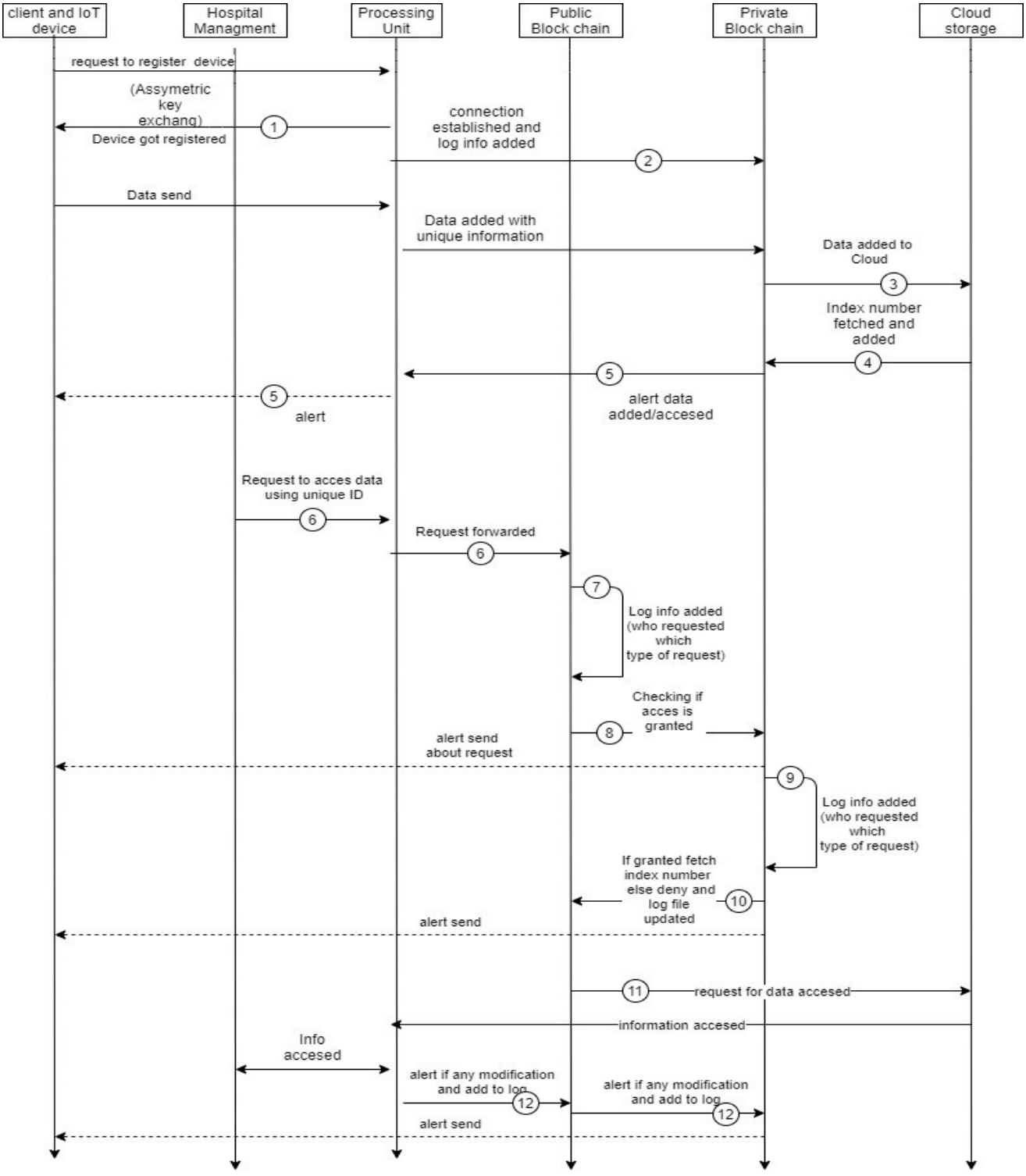

Figure 2. Time graph

IV DISCUSSION

Blockchain in the proposed framework is aimed at providing non-repudiation in the health care IoT ecosystem. The proposed model is used to provide alerts to the users whenever there is access to their data. It also maintains the log information, which can be used to retrieve information on who had an access, what kind of information was accessed and at what time. In this hybrid proposed model, patient has full control of his/her private blockchain. The private blockchain maintains all the log information and access control information for the patient's private information. If, for example, any third party tries to access information, an alert will be sent to the user. The access information will be stored in log file in the blockchain. In the same way any access from the hospital management will be tracked in log files in both private and public blockchain system and an alert will be sent to the user about any kind of authorized or unauthorized system access. User may choose to ignore usual access patterns and tune the system to raise an alarm for unusual access patterns. Moving further, not every system is fully secured, there can be some area in proposed system where malicious attacker can perform some potential attack. Some of them are as follows:

Potential Attack Scenarios:

a) Unauthorised Access to Patient Data from Hospital Employees

If an unauthorised person tries to access the patient information from hospital side, first the request is generated as shown in the step (6) on Figure 2. At the same time a log information will be added in public blockchain ledger as shown in step (7): who, when and what has been accessed. Any kind of access to the data will generate an alert to the client as shown in Figure 2 as in step 5 and by dotted lines. The stored log information in blockchain ledger system can be used later to track access details and use them in investigation process. One of the key features of the blockchain is that once the data is added to blockchain ledger, it cannot be deleted or changed, so blockchain is very reliable to track the access log added to it and helps to have a good data repudiation mechanism.

b) Unauthorized Access from Client Side

In the same way on the client side if someone tries to access data on the cloud through unauthorised access to device or processing unit on client side, the log information will be added in private blockchain as shown in step (2) and alert will be sent to the client as in step (5). The patient has full control to his private blockchain and can retrieve this log information at any time. So, the model follows a detective control mechanism related to data access and notify the user whenever there is access to the data. The saved information in form of log information in blockchain system finally provides non-repudiation mechanism.

c) A Potential Attack on Processing Unit

Processing unit is the only node which connects the client and hospital management with their respective private and public blockchain. Any attack on the processing unit can hinder the flow of information. The malicious script, if gets executed on a processing unit, can halt the flow of data to blockchain and can lead to denial-of-service attack (DoS). Moving further, if an attacker tries to access data, then that access will be recorded in the ledger. Moreover, records in the cloud are signed with the device key from which any non-authentic change in data can be tracked.

d) Susceptible Attack on Blockchain

Although blockchains are considered to be secure storage mechanisms, but at least in the pre-quantum computing cryptography world, they can be susceptible to some design attacks. One of them is the 51% attack also known as majority attack or double-spend attack. This occurs when an attacker controls over 50% of total computing power on the blockchain and is able to prevent new transactions to occur. By this attack, the malicious user is able to form block at a faster rate and by the longest chain rule the Ethereum network is forced to choose the attacker forged blockchain. Although 51% can occur but the probability of execution rate is very low and is difficult to achieve as an attacker needs lots of computing power to suppress the blockchain and decipher the hashes to become a majority player to own a blockchain, so block chain is still a secure technology.

The other kind of susceptible attack is the Sybil attack on the blockchain. In this, an attacker can control the blockchain by creating a large number of fake nodes and push the legitimate nodes in the minority which can lead to a 51% attack [14]. These virtual nodes can act like genuine nodes and can overload the network. This attack leads to DoS or DDoS attack, which can stop the working of a model. This type of attack is feasible on the blockchain which are public and are open to scan. It can be mitigated by having the complex algorithm working on the public blockchain to prevent attacker from adding new nodes.

d) Data Injection Attack on the Cloud Repository

Cloud repository is used to store all the essential data regarding client whereas blockchain is used as a secure channel. Cloud computing is considered a secure channel to save data, but these are still vulnerable to some attacks. One of it is the data

injection attack, which allows attacker to manually send queries to database in attention to access private data or to modify it. In the proposed model, it is difficult to execute because to perform this type of attack, the attacker first has to get access privilege in private blockchain, then only attacker can access data or the malicious attacker has to find a different unsecured network connection (other than the Ethereum network) to data repository, which might allow them to connect to cloud remotely and allow them to perform the data injection queries, so that they can have access to patient data.

The efficient blockchain protocols which are suitable to maintain the high load systems are important to successfully implement this model. The proposed framework generally records all the log information in the blockchain which provides non-repudiation and sends notification to the client if there is any unauthorized access to the data. Moving further, public block chain is more vulnerable to malicious attack like Sybil and 51% attack because of its public nature, which allows attacker to access it for reconnaissance scan. However, private blockchain is only accessible to the client, which makes it immune to these types of attacks. If any of the blockchains is successfully attacked by the malicious user, one should discard that blockchain and start using a new one and try to restore data from remote recovery system. After the brief analysis of different types of attack scenarios discussed above, it can be said that if the proposed architecture is accompanied by a proper protection mechanism on each node to address the related attacks, then this framework can be seen as a reliable secured system which can provide data traceability, accessibility and non-repudiation.

V CONCLUSION

In this paper, the framework regarding integration of IoT medical devices with blockchain technology in the medical sector is purposed. This framework contributes to the data protection in hospital management sector. The proposed model provides the non-repudiation mechanism by maintaining log information in the blockchain and by generating alert notification to the data owner whenever there is access to the data in the cloud depository. It provides non-repudiation in a way that it will not allow any party or person to deny the fact that they have accessed the data. The framework uses two blockchains, public and private. Both blockchains maintain the log information regarding who accessed the data at what time and maintain the event information. The framework will work if a proper protection mechanism is followed to have independent distributed nodes in order to avoid 51% attack. The private blockchain also maintains the accessibility information which is defined by the client and allows only those with the privileges to access the data.

The proposed model can be used by developers to provide detective control mechanism regarding the risk related to medical data access of the people. It provides developers a mechanism to detect, notify and verify any unauthorized access to the data, hence offers non-repudiation. A group of expert developers is needed to implement this framework to its full extent.

REFERENCES

[1] F. Hudson and C. Clark, "Wearables and Medical Interoperability: The Evolving Frontier, in Computer, vol. 51, no. 9, pp. 86-90, September 2018.URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8481273&isnumber=8481245," vol. 51, no. 9, pp. 86-90, 2018.

[2] . M. Wu and J. Luo, "Wearable technology applications in healthcare: A literature review," *Online Journal of Nursing Informatics (OJNI),* vol. 23, no. 3, 2019.

[3] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal,* vol. 16, no. 5, pp. 1368-1376, 2016.

[4] G. Aroganam, N. Manivannan and D. Harrison, "Review on Wearable Technology Sensors Used in Consumer Sport Applications," *Sensors,* vol. 19, no. 9, p. 1983, 2019.

[5] F. N. RELEASE, "FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps," U.S Food & Drug, 27 june 2019. [Online]. Available: https://www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain. [Accessed may 2020].

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: www.bitcoin.org.

[7] L. A. Linn and M. B. Koo, "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research," *U.S. Department of Health and Human Services,,* pp. 1-10, 2016.

[8] G. Irving and J. Holde, "RETRACTION: How blockchain-timestamped protocols could improve the trustworthiness of medical science," *F1000Research,* vol. 6, p. 805, 2017.

[9] S. Fujimura, H. Watanabe and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on Blockchain," *5th IEEE Int. Conf. Consum. Electron. - Berlin,* pp. 345-346, 2016.

[10] U. Goel , R. Ron Ruhl and P. Zavarsky, "Using Healthcare Authority and Patient Blockchains to Develop a Tamper-Proof Record Tracking System," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity)*, 2019.

[11] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview (NISTIR-8202)," *NISTIR,* p. 59, 2018.

[12] K. N. Griggs, . O. Ossipova, P. C. Kohlios, A. N. Baccarini, E. A. Howson and T. Hayajneh , Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring, J Med SySt., 2018.

[13] IPFS, "IPFS powers the Distributed Web," Protocol Labs , [Online]. Available: https://ipfs.io/. [Accessed 20 11 2020].

[14] P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors,* vol. 12, no. 1, pp. 55-91, 2011.