Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Chapter 14

Blockchain-based health care monitoring for privacy preservation of COVID-19 medical records

J.V. Bibal Benifa[1], G. Venifa Mini[2], Saravanan Krishnan[3]
[1]*Department of Computer Science and Engineering, Indian Institute of Information Technology, Kottayam, Kerala, India;* [2]*Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Nagercoil, Tamil Nadu, India;* [3]*Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, Tamil Nadu, India*

Chapter outline

Blockchain for Smart Cities. https://doi.org/10.1016/B978-0-12-824446-3.00005-3

1. Introduction

In December 2019, the pneumonia infection caused by coronavirus (COVID-19) occurred in Wuhan, China and spread rapidly in Wuhan areas and beyond (Wang, Hu, Hu et al., 2020). Potential stresses are now increasing on the global health care system. As the world fights the COVID-19 pandemic and its consequent economic and social effects, many governments and organizations around the world are joining the fight to minimize the spread of the virus while working fastidiously to develop a cure and a vaccine (Atri et al., 2020). Most of the countries are facing a dramatic spike in the number of medical patients, and it is very difficult to access primary doctors or caregivers. During COVID-19, the growth of IoT and wearable devices has increased the quality of patient care through remote health monitoring (RHM). In this pandemic situation, RHM is encouraged to provide self-distance and treatment outside hospitals. It also helps doctors (health care providers) to treat more patients. Using this ease of service, patients can remain linked to health care providers as needed. This also greatly reduces the medical costs and enhances the quality of health care.

The important components of RHM include monitoring devices, health data transmission to smart contracts, a smartphone with internet connectivity, and an application. This procedure is presented in Fig. 14.1, where the smartphone is a device that is used to fill the gap between individuals and organizations, and they could play a major role in resolving COVID-19 reactions. New technologies like blockchain have helped to diagnose many infected people, recognized in the areas in which COVID-19 spreads, and information can be tracked dynamically. In RHM, wearable devices and IoT play an important part to build secure medical records in smart cities. Wearable devices capture health data from patients and send it to hospitals to promote health monitoring, diagnosis of diseases, and medication.

In the health care systems, wearable devices are smart electronic devices with microcontrollers that can be implanted into clothing or attached as accessories on the body. They are seamless, user-friendly, and linked to advanced features such as wireless data transfer, real-time input, and system

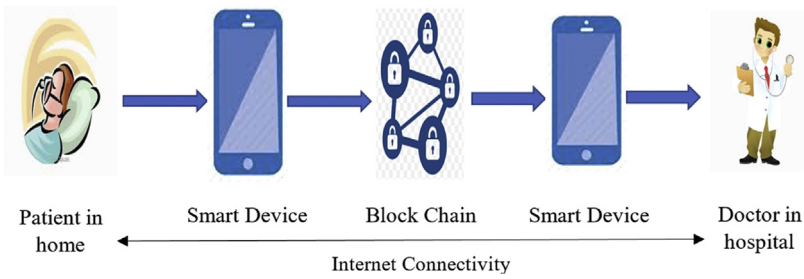

FIGURE 14.1 Remote health monitoring system.

built-in alerting mechanisms. These devices may provide health care providers with vital information such as blood pressure, blood glucose levels, and breathing habits. New wireless sensor wearable device be seated softly on the throat to track fever, cough, and respiratory activity shown in Fig. 14.2. The lightweight, flexible, and waterproof thin device about the size of a postage stamp sits just below the suprasternal notch and the noticeable dip at the base of the throat. The system tracks coughing intensity and patterns, movement of the chest wall, respiratory sounds, heart rate and body temperature, including fever, from this position. This is the first wearable device that keeps track of monitoring COVID-19 symptoms.

Health care devices can be divided into four different categories as illustrated in Fig. 14.3. Fixed medical devices can be fixed on a physical location. Medical implanted devices can be positioned inside the body. Wearable medical devices can be prescribed by doctors (health care providers). Consumer products like Fitbit and Fuelband are also used as wearable health monitoring devices.

IoT devices are embedded with software, electronics, sensors, actuators, and networking that enables the wearable user to link and share data (Haleem, Javaid, & Khan, 2020; Li et al., 2020). IoT devices are the combination of smart devices and sensors, and they have limited storage and computational resources. Smart cities trust deeply on sensors to observe parameters such as temperature, humidity, allergens, noise, traffic conditions, and power grid status. Such parameter values provide a context that helps to understand a citizen's state at any given time (Solanas et al., 2014). Further, responding to sensed data is strategically helping to make smarter health care services. By having access to this real-time COVID-19 information, the public services can react quickly to urgent health requirements and take decisions in critical situations. All countries, including India, are struggling with COVID-19 in the current pandemic situation and are still looking for practical and cost-effective

FIGURE 14.2 New wearable device.

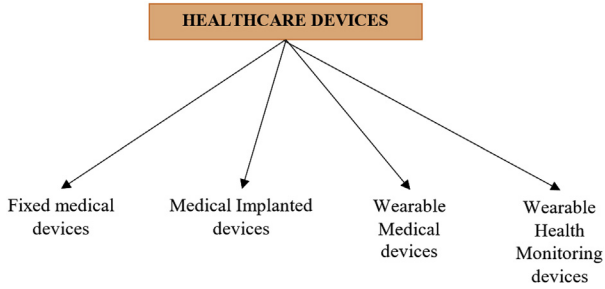

FIGURE 14.3 Health care devices.

solutions to the problems that arise in several ways. In the current typical case, almost all of the issues occur because of inadequate accessibility to the patients, which is the second most significant issue after the vaccine production question (Wang, Hu, Li et al., 2020). Using the IoT concept makes the patient's accessibility quite useful, which ultimately helps to give them substantial care so they can get out of this disease. One significant role of IoT is to acquire data through sensors and smart devices, which can be further processed and analyzed in cloud environments.

The proposed way of collecting and analyzing data from patients helps to improve the health of the civilization during this COVID 19 pandemic. Health care devices are utmost important to observe the symptoms of the patients in home by the wearable devices. The data collected by health care devices are protected and transmitted in a secure way. This will be achieved by cryptographic primitives. IoT devices encrypt the data and send it to cloud servers. The metadata of the original data is stored in blockchain. Thus, there has been a step toward combining IoT and the cloud to outsource data collection, processing and sharing capabilities.

Data Owner 1 (DO1) can store and share the data collected through the cloud with Data Owner 2 (DO2) to decrease costs as highlighted in Fig. 14.4. Since the cloud is semitrusted, there is a concern that user's data and privacy

FIGURE 14.4 Sharing of data between DO1 and DO2.

can be leaked and breached in or outsiders. Though there are many techniques for privacy-preserving data processing using cryptographic access control tools in cloud storage, these access policies and data can be tampered with and breached by cloud service providers (CSP) or by data users (DU).

Data is an extremely important currency. Health care systems accumulate tons of sensitive information about individuals. Unfortunately, the data attracts hackers. The data is accumulated in one location and it is very easy for hackers to steal the data. When it comes to data, existing technologies use centralized storage. This can be changed in the future by storing data in a decentralized way. The decentralized way of storing data is achieved through the blockchain, becoming popular in the near future. Due to the decentralized existence of blockchain technology, hackers no longer have a single entry point, nor are they able to access entire databases in case of stealing data. Blockchain-based technology can also safeguard all data exchanges between IoT devices. It can be used to achieve safe data transfers near real-time and to ensure timely contact between devices located thousands of miles away (Jesus, Chicarino, Albuquerque, & de Rocha, 2018; Rifi, Agoulmine, Chendeb Taher, & Rachkidi, 2018).

The blockchain's irreversibility property becomes a resistance to a consent revocation feature, which allows users to deny permission for designated individuals from a certain action on the data. Blockchain's transparent property allows all network participants to view all data that can create a question of confidentiality. Blockchain's restricted storage becomes an issue toward the ease of use for the exponential growth of the different medical related data. Although private blockchain like Hyperledger Fabric (Nasir, Qasse, Abu Talib, & Nassif, 2018) have the potential to control the contribution in its blockchain network, the personal health record system gives access to a particular part of the system only to certain individuals. Due to that, a privacy disclosure is also an issue.

This chapter aims at resolving these blockchain disadvantages in smart cities and proposing an RHM model based on blockchain to solve issues in this pandemic situation. The proposed system is constructed using blockchain technology on IoT to reduce the probability of transmission, and increasing the possibility of better results. Proxy reencryption (PRE) and other cryptographic methods are used for privacy protection to protect the sensitive information of users. In other terms, users should determine individually who should access their data without violating the privacy of their data and identity.

The key contributions of this work are summarized as follows.

IoT device data were initially encrypted by advanced encryption standard (AES). Then, it is integrated with GateWay server (GW) to verify the validity of all authenticity and behavior inside the system.

Blockchain can be used to establish a privacy scheme that protects patient health information to promote the concept of nonrepudiation, transparency, and tamper resistance.

An access control framework is proposed by the use of PRE techniques to support features of fine-grained access control and consent revocation, while cloud storage is used to support the availability function.

The remainder of the chapter is structured according to this summary. Section 2 presents the background of blockchain and issues in the existing technologies, attribute-based encryption (ABE) and conventional health care systems on cloud environments. The proposed model is defined with a detailed architecture in Section 3. Section 4 investigates the safety measures and privacy of the proposed model, and Section 5 evaluates the efficiency and the discussion on the results is presented in Section 6. Finally, the chapter is concluded in Section 7.

2. Background and related works

Blockchain is an open, distributed ledger that can verifiably and permanently record transactions between two parties. It allows organizations to communicate without a central, trusted third party (Mayank, Danilo, & Katina, 2019).Furthermore, blockchain provides smart contracts without any key authority. At this date the blockchain Ethereum is the main facilitator of blockchain smart contracts (Buterin, 2014). A Blockchain is a diary which can be forged hardly. The main attribute of blockchain is decentralization, which means the information applied to blockchain is not regulated by any central authority. The blockchain consists of a number of nodes. A node is a virtual machine or physical machine. The entries sent to the blockchain are accepted in a peer-to-peer network using different consensus protocols. The protocols are designed by blockchain creators. One node can be identified by its unique IP address. Blockchain can maintain privacy in both the public key and private key. The user enters into the blockchain through public key cryptography and the messages are authenticated with a private key. Users interact without any clear reference to their identity with their private key and public key. Another main function of blockchain is that of persistence. Owing to the distributed ledger, maintained through several nodes (Zheng, Xie, Dai, Chen, & Wang, 2017), it is almost impossible to delete entries after being accepted into the blockchain. In addition, the prospect of anonymity is an attractive feature found in many blockchains.

Fig. 14.5 presents the basic structure of blockchain. A block is a basic element, which stores transactional data in the blockchain system. A block in the blockchain contains two parts, namely, header and body. The header of the block contains block number, hash code, previous block hash, nonce, metadata, timestamp, and Merkle root. The body of the block contains transactions and transaction counters. Each block is cryptographically connected to other blocks (Merkle, 1989). The blockchain retains an ever-growing collection of data entries, packed together into data blocks. Such data blocks are readable by all, viewed by everyone in the network, writable by everyone, and verifiable by

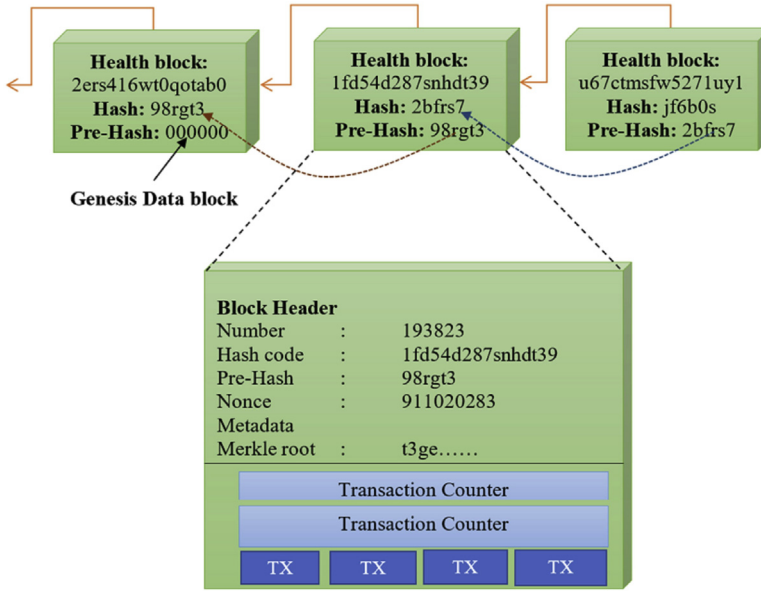

FIGURE 14.5 Basic structure of blockchain.

all. This allows decentralized data management and transactions. These properties of the blockchain receive a lot of publicity in various applications.

Blockchains allow traceability by linking a new block to the previous one using hash, and thereby creating a chain of blocks. The block transactions are generated in a Merkle tree (Merkle, 1989) as shown in Fig. 14.6, where each value of the leaf can be checked to the known root.

Au et al. (2010) offered a positive response to this issue by bringing forward a general structure for safe sharing of personal health records (PHRs). This program allows patients to securely store and share their data on the cloud server (such as their caregivers) and, in turn, practicing doctors can refer the

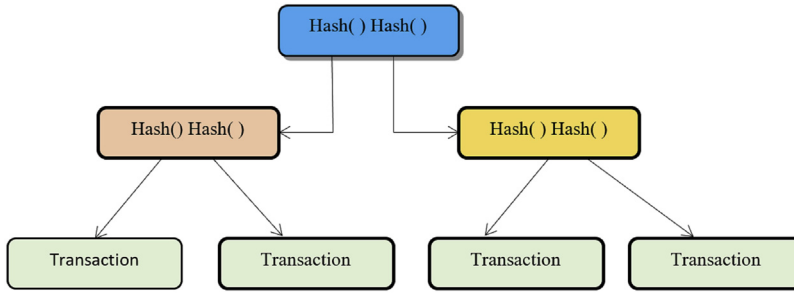

FIGURE 14.6 Merkle tree of transactions.

medical records of patients to specialists for testing purposes if appropriate, while ensuring that patient information remains confidential. Cloud technology has been seen as a popular candidate for the storage of confidential medical records in India, but the security protection given to date is still inadequate without affecting the practicality of the system.

Kaufman (2009) proposed an idea of data security in the world of cloud computing. Today, within the confines of the internet, a practice known as cloud computing technology enables use of scalable, distributed computer environments. In this modern computing environment, users are uniformly expected to acknowledge the principle of trust that underlies it. The virtual environment enables users in the cloud computing world to access computational power that exceeds that found within their own physical worlds. The data in a cloud vary from publicly accessible sources with minimal security issues to private data with highly confidential information. Like with other developments in technology, regulators are usually in a "catch-up" mode for defining regulation, governance and law. Cloud computing provides an extension of previously encountered issues with the internet. To ensure that these decisions are knowledgeable and suitable for the cloud computing environment, the industry itself should develop consistent and efficient policy and governance to define and enforce acceptable security methods.

Wangthammang and Vasupongayya (2016) suggested a centralized storage system for encrypted personal health record data for cloud storage purposes to handle encrypted PHR data. It offers an API for the upload/download of encrypted PHR data from a cloud storage network. The distributed storage design for encrypted personal health record (DSePHR) addresses Hadoop distributed file system (HDFS) namode memory problems by classifying the encrypted PHR data into small and large files while storing a lot of small files. HBase schema which is proposed in this work should manage the small files. The memory use and processing time of the proposed DSePHR was measured using actual data sets from various health care populations.

Liam, Buchanan, Jonathan, & Owen, 2018 addressed recent work in the fields of traceability, data sharing, clinical trials and methods for monitoring medications. There are many health care and wellbeing fields that could be improved using blockchain technology. Those include computer monitoring, clinical trials, prescription monitoring and insurance coverage. Hospitals may trace their properties through a blockchain network, and over a system's entire lifecycle, via patient monitoring. The collected information will then be used to enhance patient safety and include postmarket analyses to increase productivity savings.

Ivan (2016) addressed blockchain as an innovative approach to safe data storage for safety, implementation hurdles, and a strategy for increasing change from current technology to a blockchain solution. Various methods of capturing and exchanging medical data have a range of drawbacks that restrict patient access to their clinical information, minimize the availability of critical

data to care providers and eventually pose an obstacle to turning US health care into a learning health system. These shortcomings can be remedied by storing patient health care data within a blockchain-based storage scheme.

Dubovitskaya, Xu, Ryu, Schumacher, and Wang (2017) proposed a system for the management and exchange of electronic medical records (EMR) data in patient care for cancer. Electronic medical records (EMRs) are important, highly confidential private health care information, and also need to be shared among peers. Blockchain offers a common, permanent, and transparent history of all transactions to create secure, accountable, and open applications. This presents a unique opportunity to build a stable and dependable EMR data management and sharing framework using blockchain. This proposed research will dramatically reduce the processing time for exchanging EMR, enhance patient care decision making, and minimize total costs. Kosba, Miller, Shi, Wen, and Papamanthou (2016) presented Hawk, a decentralized smart contract program that does not explicitly store financial transactions on the blockchain, thereby protecting the public's transactional privacy. A Hawk programmer can write an intuitive private smart contract without cryptography, and the compiler automatically generates an effective cryptographic protocol where contractual parties communicate with the blockchain using cryptographic primitives such as zero-knowledge proofs. To formally define and explain why these protocols are safe, the blockchain cryptography model was formalized. Nonetheless, existing systems lack transactional privacy. All transactions are revealed on the blockchain, including the flow of money between pseudonyms and the sum transacted.

Radanovi and Liki (2018) explored the possibilities of medicine for using blockchain technology. Cases of this technology have so far been used for cryptocurrency, digital contracts, financial and public records, and ownership of assets. Future uses are expected to spread to medicine, technology, education, intellectual property, and supply chain management. Blockchain technology is a decentralized database that stores a record of assets and transactions through a peer-to-peer computer network protected by cryptography and, over time, its history is locked into data blocks that are cryptographically connected and protected together. Medicine-related technologies may include electronic health records (HER), health care, biomedical testing, product distribution and procurement procedures, and medical education. The use of blockchain is not without its limitations and at present this technology is highly unstable and lacks public or even professional information, making it impossible to have a strong strategic view of its true potential for the future. There are currently issues with the scalability, smart contract protection and app acceptance.

Marek (2018) developed a ground breaking blockchain technology concept that addresses critical data protection, implementation and integration issues, providing a new strategy for the health care sector that has the ability to link providers while protecting sensitive data. In order to ensure ease of

deployment in a hospital system, blockchain technology using a distributed architecture with microservices was built. This architecture enables user to encapsulate core functions with the system into discrete services that can be independently scaled depending on the requirements of a specific hospital system. As part of this architecture, core components for safe handling of cryptographic secrets, communicating with blockchain nodes, enabling large file sharing, allowing secondary-index dependent lookups, and incorporating external business logic that governs how users communicate with Smart Contracts (SCs). Through enabling data exchange between providers and EHR systems, blockchain technology has the ability to improve health care delivery. Major roadblocks however stand in the way of the widespread adoption of this technology in the health care industry. This blockchain-based data sharing solution solves two of the most important health data sharing problems associated with using blockchain: securing sensitive health records, and deploying and integrating blockchain applications through multiple hospital environments.

Clauson, Breeden, Cameron, and Mackey (2018) presented an overview of the opportunities and challenges associated with the implementation and deployment of blockchains for the health supply chain, focusing on pharmaceutical supply, medical equipment and services, the Internet of Healthy Things (IoHT), and the public health sector. Griggs et al. (2018) built an SC program that would enable patient tracking and medical procedures in real time by sending alerts to patients and medical practitioners, while maintaining a safe record of who initiated such activities. It will overcome several security issues associated with remote monitoring of patients and simplify the distribution of HIPAA-compliant alerts to all parties concerned. The proposed system is to use blockchain-based SC to facilitate safe analysis and management of medical sensors to handle the protected health information (PHI) created by those instruments. Using an Ethereum-based private blockchain, they built a network where the sensors interact with a mobile device that calls SCs and records all events on the blockchain.

Luis, Frank, & Ole, 2018 identified how blockchain technology can be used in public health surveillance by exchanging decentralized genomic data. A brief overview of why blockchain technologies are required in public health with a distinction between public and private blockchains is presented. Eventually, a plan for a network of blockchains is included, using the Cosmos architecture, along with decentralized storage frameworks such as IPFS and BigchainDB, to resolve the interoperability problems in the health sector. Luis, Frank, & Ole, 2018 aimed at exploring the role of blockchain in supporting data management in clinical trials and establishing proof-of-concept implementation of a patient-facing and research-facing framework. Blockchain-based SCs have been developed using Ethereum framework. The BlockTrial is a program that uses a web-based interface to allow users to run SC on an Ethereum network related to trials. Functions require patients to give

researchers access to their data and allow researchers to query data that is stored off the chain. This program creates a permanent and clear log of these and other transactions as a form of distributed ledger. It could also encourage patients to become more involved and fully informed research partners.

Khan and Khan (2018) proposed a system for validating electrical transactions embedded in blockchain using multiple producers' signatures based on their assigned attributes. Such signatures are checked and supported by users who meet certain qualities without any details being released. The producers generate the public and private keys for these consumers, and the endorsement process using these keys ensures that these consumers are approved. No central authority is required in this approach. Producers are given a hidden pseudorandom seed function to avoid collision attacks. The comparative review shows the efficacy of the proposed solution over the current ones.

Azaria, Ekblaw, Vieira, and Lippman (2016) proposed a modern, decentralized record management system for managing EMRs using blockchain technology that provides patients with accurate, unchangeable logging and easy access to their medical details via providers and treatment sites. Taking advantage of special blockchain assets, MedRec handles authentication, confidentiality, transparency, and data sharing. A modular architecture combines existing, local data storage solutions from vendors, enabling interoperability and making our system simple and adaptable. MedRec thus allows data economics to emerge, offering big data to motivate researchers while at the same time involving patients and providers in the option of releasing metadata. The purpose of this short chapter was to show a working prototype by which was being examined and discussed this approach before field tests.

The IoT systems deliver various opportunities and provide successful cyber-security solutions. It has many obstacles such as providing a secure data sharing environment and maintaining privacy because of the vast amounts of data generated by IoT devices (either single devices or whole systems). Data owners continue to think about how their data is being used when the power is out of hand. The protection of their data in cloud computing is the most prominent problem, and this affects the efficiency of this paradigm (Mineraud, Mazhelis, Su, X., & Tarkoma, 2016; Tariq et al., 2019) Encrypting data until they are outsourced has proven to be a secure way to reduce security issues. It is impossible to share the data with users when the data is encrypted as the owner needs to share the decryption key with those users, thereby providing access to the data. Another concern that emerges from sharing the keys is the revocation of accounts, where certain accounts would be refused service. What data owners normally do is invalidate the current key by using a new key to reencrypt the entire collection of data and redistribute the key to (authorized) users (Agyekum et al., 2019; Xia et al., 2017). Such action often becomes tedious and requires tremendously when large volumes of data are outsourced, and the owner does not retain a copy of the outsourced data locally.

ABE, an encryption scheme initially suggested by Sahai and Waters, achieves both access control and data protection by granting users specific access rights based on their attributes. One of their functionalities is the removal of user's access privileges. Using attribute-based encryption is also intended to provide fine-grained access control, since it decides the user has access rights to which form of data (Guo, Zhuang, Jie, Ren, Wu, & Choo, 2016). ABE is an ideal method for enforcing complex access control policies: the data to be accessed is connected to a set of attributes, and the user's rights are defined by a logical expression over those attributes (Ostrovsky, Sahai, & Waters, 2007).

Chow, Weng, Yang, and Deng, (2010) proposed an efficient one-way PRE scheme (without resorting to pairings). Under the Diffie-Hellman theoretical theory, they achieved high efficiency and CCA-security using the token-controlled encryption method in the random oracle model and a relaxed but rational definition. PRE makes it possible for a semitrusted proxy to convert a ciphertext originally intended for Alice into one which encrypts the same plaintext for Bob. The proxy just needs Alice's reencryption key, and cannot know much about the encrypted plaintext. It provides versatility in different applications, such as sensitive email, digital rights management, and remote storage.

Rao (2017) proposed a proven, secure CP-ABSC system for cloud-based PHR sharing that provides fine-grained access control, confidentiality, authenticity, sign crypto privacy, and simultaneous public verification. This system takes advantage of concise monotonous boolean functions as predicates of signing and encryption, and understands protection in the standard model. At the positive side, this construction shows a short ciphertext size and involves fewer pairing computations compared to the current regional schemes.

Li, Li, Wen, Zhang, and Zhang, (2017) presented an improved ciphertext-policy attribute-based encryption (CP-ABE) scheme to create an encrypted data access control solution suitable for mobile users in a hybrid cloud environment. In hybrid cloud computing, encrypted data access control can provide organizations with a fine-grained method of access to policies which are similar to organizational policies. This scheme is secure, versatile and efficient for use in mobile hybrid cloud computing but not suitable for IoT devices. Gu, Jia, Wang, and Wen (2017) presented an attribute-based signature (ABS) system and outlined a comprehensive ABS protection model. Under this framework, in the standard model, an ABS scheme was presented for monotone predicates, where we select the Waters' signature scheme as the prototype of our ABS scheme. ABS is a novel cryptographic primitive that can render a message signed by the signing party with fine-grained control over information identification. Many ABS schemes had been proposed at the moment but most of them are not very successful.

Sangeetha and Vaidehi (2017) proposed a secure cloud-based PHR system for the sharing of PHRs between multiple users using ABE. Patients can encrypt their PHRs in this proposed system, and store them on semitrusted cloud servers. In addition, patients can retain control over access to their PHRs by allocating rights of fine-grained, attribute-based access to selected DUs. Ateniese, Fu, Green, and Hohenberger (2006) presented several efficient proxy reencoding schemes which offer security improvements over earlier approaches. The primary advantage of this schemes is that they are unidirectional (i.e., Alice can delegate to Bob without Bob needing to delegate to her) and do not allow delegates to show any of their hidden key to everyone. Proxy positions only a small amount of trust. For example, it is not able to decrypt the ciphertexts it reencrypts, and even though the proxy publishes all the reencryption information it knows, they have proved their schemes reliable. It allows for a range of applications that would not be possible if the proxy required full trust.

Private block chain (Hyperledger) is more efficient to reduce problem in mining process. The PHR data was protected using both the ABE scheme and the semitrusted servers. An access control mechanism is created by encrypting the sensitive PHR data. It increases the computational cost with the number of not revoked users if PHR contains huge volume of data. The issues related to blockchain are identified and privacy-preserving data sharing is projected as a potential solution.

3. Blockchain taxonomy

There are three major types of blockchains (Table 14.1): public, consortium, and private (Clauson et al., 2018; Zheng et al., 2017). They have different

TABLE 14.1 Type and properties of blockchain.

Property	Blockchain of public	Blockchain of consortium	Blockchain of private
Deciding consensus	All mineworkers	Selected group of nodes	By an organization
Read permit	Public	Public or limited	Private
Unchangeability	Almost impossible	Could be distorted	Could be distorted
Effectiveness	Low	High	High
Centralized role	No	Not fully	Fully
Consensus process	Unauthorized	Authorized	Fully authorized

features about who can access, write, and read the blockchain data. Everyone can access the data in a public chain, and everyone can join in and contribute to both consensus and modify the core program. The blockchain of public is used in cryptocurrencies. Cryptocurrencies such as Bitcoin (Nakamoto, 2019) and Ethereum (Buterin, 2014) are listed as public, permissionless blockchains. A blockchain of consortium may be considered as semicentralized, with only a small number of selected groups of organizations having access to viewing and participating in the consensus protocol. A private blockchain should be used as a central network, because it is fully controlled by one organization.

3.1 Popular blockchains

Existing blockchain technologies can be used to build decentralized applications. The most popular are Ethereum (decentralized platform) (Buterin, 2014) and Hyperledger (framework) (Cachin, 2016), both enabling developers to construct new blockchain applications on existing blockchains and to develop new test chains using their protocols.

3.1.1 Smart contract

SC is a digitized transaction protocol which enforces the contract terms (Macrinici, Cartofeanu, & Gao, 2018). It has long been proposed, and now it can be implemented in block chain technology. In blockchain, SC is a fragment of code that could be automatically executed by miners. SC have transformative potential in different sectors, such as financial services and IoT. The encrypted-only design of blockchain storage is perfect for storing data to facilitate a resistance function. Keeping data access permission can cause difficulties in providing a consent revocation feature. Transactions are publicly visible in a decentralized ledger (Kosba et al., 2016). It takes a lot of time for transactions and blocks to be propagated, because there are many nodes on public blockchain network. The transaction throughput is thus minimal, and the latency is high. A decentralized block generating phase requires a large amount of computing power, and energy. Consequently, the proposed model for RHM scheme should identify a method to deal with such limitations.

3.1.2 Proxy reencryption cryptosystem as a scenario

PRE is a type of asymmetric encryption (Public key cryptosystem) that enables a proxy entity to convert or reencrypt data from one public key to another, without accessing the underlying plaintext or private keys (Nunez, Agudo, & Lopez, 2017).The ciphertext which means plaintext is encrypted under the PRE scheme. The generated ciphertext can be retrieved in such a way that it can be decrypted by another user using his or her private key even though the cipher text is not initially encrypted with his or her public key. The scheme would therefore be a useful tool for providing a secure network for

data sharing. The data owner must give the reencryption key to the proxy to transfer the data inside the proxy reencryption scheme. Moreover, the proxy will not be able to access any information from the reencryption key about the original data. The key to reencryption is generated by combining the secret key of the data owner and the public key of the intended-user. Therefore, the PRE scheme is flexible for the construction of an access control system in our proposed framework. In addition to the PRE proposal, four operations are required for the secure authentication of stored and transmitted data within the proposed framework: (1) encrypt and decrypt, (2) reencryption, (3) signing and verification (e.g., digital signatures), and (4) encryption and decryption verification.

Symmetric encryption cannot be used separately, because it means sharing the same key between suppliers, owners, and consumers. The conventional public key cryptographic system requires the data owner to be accessible online to reencrypt data when necessary. It is not always feasible, apart from being extremely inefficient. PRE can be used as a way to delegate decryption privileges, which then represents a natural candidate to create cryptographically enforced access control frameworks consistent with our motivating scenario. Moreover, the proxy cannot discover any information about the encrypted messages by any of the keys. The PRE cryptosystem is developed by Blaze, Bleumer, and Strauss, (1998). This cryptosystem contains some disadvantages of being bidirectional. Also, it is prone to collusion attacks. To resolve such a problem, the modified proxy reencryption scheme known as Ateniese, Fu, Green, and Hohenberger (AFGH) is used (Ateniese et al., 2016). Ateniese et al. work has been extremely influential as it offers the first formalizations of PRE syntax and notions of security as well as an initial description of PRE properties. The authors also offer multiple PRE applications, and in particular an access control server for a reliable file system. PRE enables the sender to encrypt the data just once and assign access to the data depends upon public keys for the recipients. This eliminates the data owner's requirement to be online, and also supports access revocation. The important properties of AFGH are (1) unidirectional ($X \rightarrow Y$ reencryption does not allow $Y \rightarrow X$ reencryption); (2) antiinteractive (trusted third parties' interactions does not require to generate a key for reencryption); (3) access (the reencrypted ciphertext will be decrypted by delegator); (4) optimal key (secret key size remains constant, whatever the number of delegations accepted); and (5) nontransitive (proxy alone cannot redelegate the right to decrypt). Such properties are suitable for the proposed model. The AFGH reencryption scheme will thus be used to establish the access control within the proposed model.

Fig. 14.7shows the correspondence between main actors in PRE. Alice (the data owner or sender) will assign decryption rights to Bob (the recipient or receiver) through a reencryption process performed by a group of reliable-minimized peers for any ciphertext designated for her. The delegator is

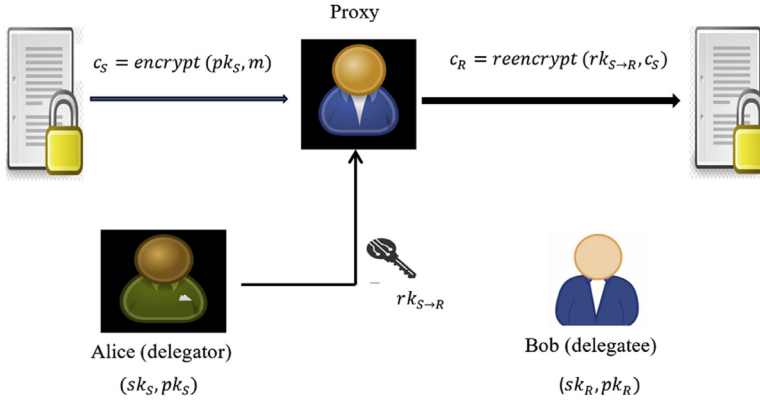

FIGURE 14.7 Correspondence between main actors in PRE.

Alice and delegatee is Bob. Delegator is the actor, who delegates his rights of decryption using proxy reencryption. The delegatee is allowed a reserved right to decrypt ciphertexts that were reencrypted for him with the permission of the original recipient, but not intended for him in the first place. Here, the encryption algorithm *encrypt* generates a ciphertext c_S when entering the public key pk_S and m message file. The reencryption algorithm *reencrypt* generates a second ciphertext c_S when a reencryption key rk_S and a ciphertext c_S is entered as input. By performing reencryption, Bob will combine these separate reencryptions and decrypt the original message using his private key sk_R.

3.2 Remote health monitoring on cloud

RHM is a technology that allows patient monitoring beyond traditional clinical environments, such as at home or in remote areas, which can improve access to treatment and decrease the costs of providing health care. In the medical sector cloud computing is rapidly becoming a requirement. It could be the solution to improve health care by exchanging patient details on urgent cases in real-time between medical providers. The deployment of the health record in a cloud environment provides many opportunities such as inevitable usability, versatile computing resources, high degree of intrusion detection and information sharing with other systems. As per HIPPA, the cloud providers are considered as noncovered organizations.

Like the other digital medical record system, health record data is handled and operated by the health record owner. The owners of health record can share their health data with others selectively while keeping other parts private. The cloud platform allows health record data to be accessed anywhere at every time. The health record program can also be assisted by the cloud to plan for medical appointments and create a more comprehensive image of personal health for communication, collaboration, and interaction.

3.3 Cryptographic primitives

The significant part of the proposed scheme depends upon pairing-based cryptography and cyclic group can be provided by bilinear mapping method. Let be a group which contains a collection of elements with binary operation, The properties of these primitives are presented as.

Closure property: Closure means an additional element in the set is the product of performing the operation on any two elements in the set. $\left(x, y\ \varepsilon\ G,\ \forall_{x,y}\ \varepsilon\ G\right)$.

Associative property: The order of the elements does not matter. $(x.y)z\ =x.(y.z),\ \forall_{x,y,z}\ \varepsilon\ G$.

Identity property: This property describes that $i\ \varepsilon\ G$ such that $x.i\ =x\ =i.x,\ \forall_x\ \varepsilon\ G$.

Inverse property: This property describes that $x^{-1}\ \varepsilon\ G$ such that $x.x^{-1}\ =i\ =x^{-1}.x,\ \forall_x\ \varepsilon\ G$.

The operations involved in group G are additive, multiplicative, or mapping function.

3.4 Bilinear mapping method

Let us define G_0 and G_1 as two cyclic groups on $F(Q)$, G_m is a multiplicative group with order of prime number q. The bilinear mapping method $e:\ G_0\times G_1\rightarrow G_m$ is a function, which should accept following properties.

Bilinearity: $\left(e\left(x^a, y^b\right) = e(x,y)^{ab}\right)$ such that $\forall\ x\ \varepsilon\ G_0,\ y\ \varepsilon\ G_1,\ a,\ b\ \varepsilon\ Zq$.

Nondegenerate: if $G_0\ =<x>,\ G_{1=}<y>$, then $G_m\ =<e(x,\ y)>$

Efficient Computability: $\forall x \in G_1,\ \forall y \in G_2$ for any two elements x, y. This can be efficiently computed using $e(x, y)$.

4. Proposed work

Fig. 14.8 illustrates the architecture of an IoT-based remote health monitoring system that can be used in smart cities or the home. In these systems, information related to patients are recorded by body-worn or implanted sensors, in which the patient is prepared to monitor multiple metrics in a personal way. IoT is an advanced technology that ensures quarantine for all infected persons suffering from this virus. This is beneficial for a secure monitoring system during quarantine. Using the internet-based network, all high-risk patients are easily monitored. This system is used for measuring biometrics such as blood pressure, heart rate, and levels of glucose. Data obtained from IoT devices will help doctors to diagnose patients with the appropriate treatment plan and achieve the desired outcomes. Because of the sensitivity of the health record, the data should be protected at rest and on transmission using cryptographic primitives.

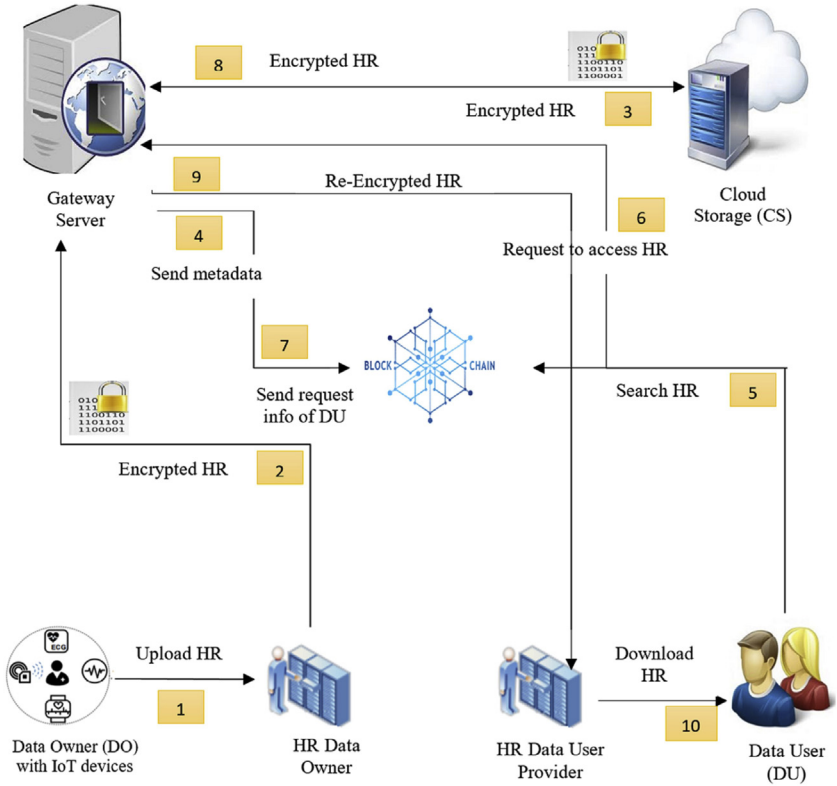

FIGURE 14.8 Architecture of an IoT-based remote health monitoring system.

The health record is exchanged through a proxy reencryption mechanism. The reencryption keys and other information required for the authentication process will then be stored on the gateway server proxy. Health record metadata will be stored on a private blockchain to enable search and resistance characteristics. The health record can be used by other health record owners such as health care providers, e.g., physicians and nurses. The following six major entities will be part of our model.

4.1 IoT devices

The IoT-enabled devices have made remote monitoring possible in the health care sector, the ability to keep patients safe and secure and inspiring doctors to provide untouchable treatment. The interaction between patient and doctor has become efficient and easier. IoT has changed the lives of people, especially corona patients, by allowing for continuous monitoring of health conditions. It has a huge influence on the people and their families quarantine in this

pandemic situation. Monitoring system sends alerts to family members and health care providers concerned about any disruptions or changes in a patient's daily activities. The spreading of infections is of serious concern to hospital patients, who will be in active infection. Hygiene monitoring IoT devices helps to prevent patients from being contaminated. Patients are the owners of their medical data and are responsible for authorizing, refusing or revoking access to data to any other entity, such as health insurance or health care providers.

4.2 Data owner (DO)

The data owner (DO) is a person possessing the health record (HR) data and required to access or store their health data. DO has full control over its HR results. DO must specify an access control policy for its HR data, and DO can allow or disallow such access permissions on its HR data to others. DO must then create the reencryption keys and the metadata for its HR. DO may also allow some users to add more data on their behalf and DO may re-check access to the newly added HR data.

4.3 Data user (DU)

The Data User (DU) is an entity that demands access to the HR data with the corresponding DO authorization. DU may include health care professionals, health insurance companies, and caregivers from many categories. DU can scan and get the metadata through the blockchain, and can later request the gateway server about HR information. DU can create/upload new HR data into program with a delegated authority.

4.4 Gateway server (GWS)

The duty of the gateway server (GWS) is to verify the validity of all authenticity and behavior inside the network. These activities include reencrypting the HR files, storing the metadata, and accessing the stream log. The private blockchain is also operated by GWS. All communications between GWS and other entities are made through a secure SSL/TLS channel. GWS is considered to be a semitrusted server in this work; the server obeys the procedure specified in the work but is curious to know the data.

4.5 Blockchain network

The blockchain network will make the transition from medical interoperability to patient-centered interoperability. It is defined as a private blockchain. The trusted third parties such as hospitals, institutions, researchers, and government agencies have the power to manipulate the blockchain within a private network. Blockchain technology enables patients to delegate access rules for

their medical data. For instance, allowing different researchers to access portions of their data for limited span of time. Patients can connect to other hospitals with blockchain technology, and collect their medical data automatically.

4.6 Cloud storage (CS)

Cloud storage (CS) is responsible for storing real PHR data that is encrypted. CS is also called a server with a semitrusted feature. The data owner and users (data subjects) must enroll with the IoT gateway server for registration to make an initial agreement. The private and public key of the owner and users are generated by bilinear mapping function. The generation of key pair is based on the cyclic groups G_0 and G_1 with order of prime number q for the mapping function $e : G_0 \times G_1 \rightarrow G_m$. Let $x \in G_0$ and $(x, y) \in G_1$ be the parameters of system. A randomly selected number $a \in Z_q$ is taken as private key sk. The public key is generated with computation $pk = x^a$. The private key is preserved locally and the personal identifiable information and public key is transferred to the gateway server for registration. The enrollment details for registration is stored by gateway server and provide access control privileges for the data subjects are stored in Hyperledger (private blockchain). As a patient-centric system, RHM provides patients with a detailed view of their medical record, restoring authority through interaction. It facilitates information collection, alteration, generation and review, maintains data integrity, authenticates sense of identity, encourages unambiguous exchange, and executes access rights given to users through SC. RHM is not designed to replace PHRs, but to serve as a gateway between patient and trusted parties.

4.7 Uploading HR to cloud

The procedure for storing a HR or medical data in the proposed model is shown in Fig. 14.9.Patient created his/her own medical data (m) by acquiring data through IoT devices and responsible for allowing or denying access to data. Once it is created, patients connected to the HR data owner provider and submit the medical data with updated information. The consistency, reliability and accuracy of data should be secured over its entire life cycle. To maintain the consistency of data, the message digest $mdig = msgdig(m)$ is computed using SHA-2 hashing algorithm. Message digests are used to preserve the integrity of a piece of data to detect modifications and alterations to any part of a document.

Public key cryptography is used to convert the medical data to encrypted form. According to HIPAA act, the health information of the patient should be encrypted before transmission. As per the guidelines of National Institute of Standards and Technology 800-11, the AES, or any public key cryptography is applicable for data encryption. Traditional AES and public key cryptography

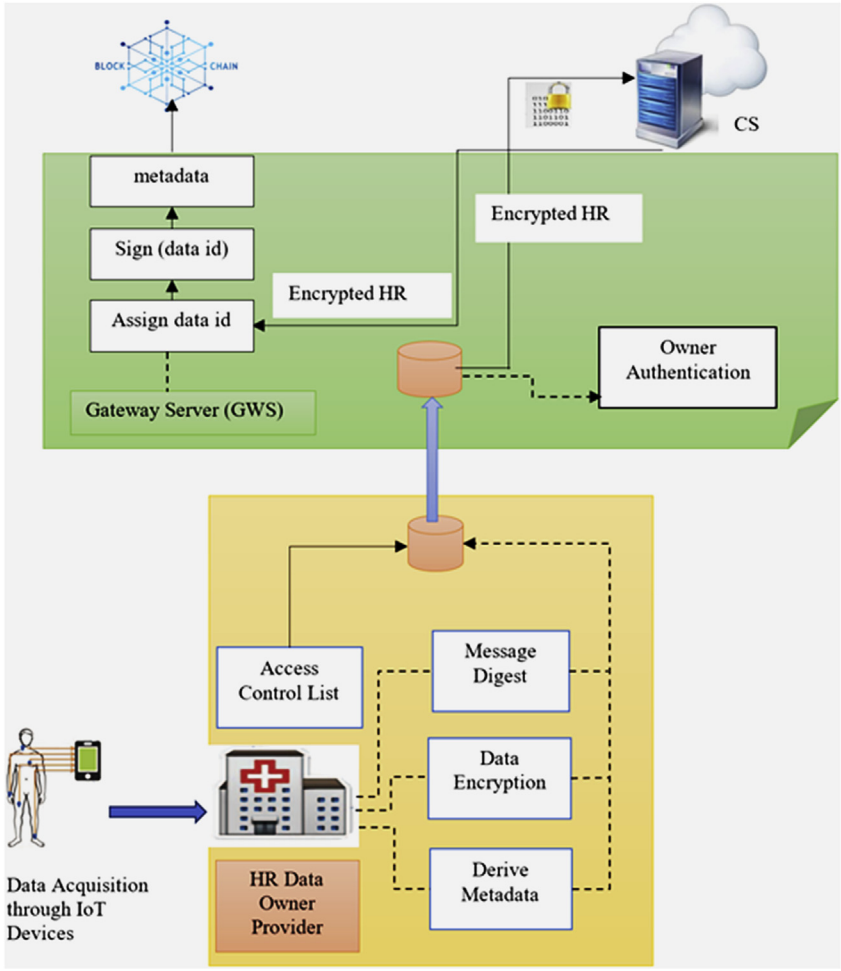

FIGURE 14.9 Uploading HR to cloud.

are infeasible for IoT devices. In the proposed model, PRE is acceptable as a public key cryptography. The medical data of the patient are encrypted by the public key pk_S and exchanged without revealing sensitive information. Encryption provides the data privacy and data confidentiality. The ciphertext is calculated using $c_s = encrypt(pk_s, mz^n)$, where '$n$' is a random element and $pk_s = x^{an}$.

A record of medical data can be searched by means of metadata. Patient metadata consists of message digest, owner identification, digital sign, type and format, date, description and data identifier. To ensure the authenticity of the message, digital signature is generated using data owner's private key

$digsign_{sk_s}(mdig)$. For each person who is permitted to access the medical data, the reencryption keys are created and the individual will be included in the access control list (ACL) for exchanging sensitive information.

Each reencryption key is derived from the private key of the owner sk_S and the respective public key of user pk_R. For example, Alice sends the reencryption key $rk_{S\to R} = x^{b/a} \in G_0$ to Bob, where a is the secret key of Alice and x^b is the public key of Bob. Then a package of encrypted medical data c_s, message digest *mdig*, digital signature *digsign*, patient metadata and ACL are transferred to the GWS.

The important job of GWS is to verify the digital signature of owner for authentication. Then the encrypted medical data is uploaded to CS. A link (lk) is created and it is connected to the encrypted data block. Gateway server creates a data identifier (md_id) and it is assigned to data block. After the assignment, it is mapped to the link (lk) of data, which resides in CS. The information about link (lk) data identifier (md_id), ACL (ACL) are stored in gateway server. Then the gateway server generates its data identifier signature. All the information namely patient metadata, owner digital signature, message digest, data identifier and server data identifier signature is transferred to private block chain.

4.8 Downloading health record

The DU downloaded the data by getting the information of the requested data through the patient metadata stored in private blockchain Fig. 14.10. The gateway server verifies and validates the user with the help of his/her signature. Also, it verifies the timestamp appended with data identifier by the user. When the user is authenticated, the gateway server retrieves data identifier from the local storage using the (md_id), and retrieves the requested encrypted medical data from the CS.

Before transmitting the encrypted data to the user, it should be reencrypted by gateway server. The gateway server derives the reencryption key to change the encrypted data of owner to ciphertext that is to be decrypted by the user. For instance, Alice original ciphertext can be reencrypted to ciphertext that is to be decrypted by Bob, the reencryption key is obtained from ACL maintained by gateway server $rk_{S\to R} = x^{b/a}$. Alice's original cipher text $c_s = encrypt(pk_s, mz^n)$ is converted to $c_R = \left(mZ^n, Z^{bn}\right)$, where $Z^{bn} = e\left(x^{an}, x^{b/a}\right)$. The reencrypted ciphertext is transferred to Bob. Bob uses his private key sk_R to decrypt the ciphertext.

4.9 Data user revocation

The revocation of a user is included in the RHM system. CS is available for the storing of real encrypted HR files. The authenticated HR is queried by all users

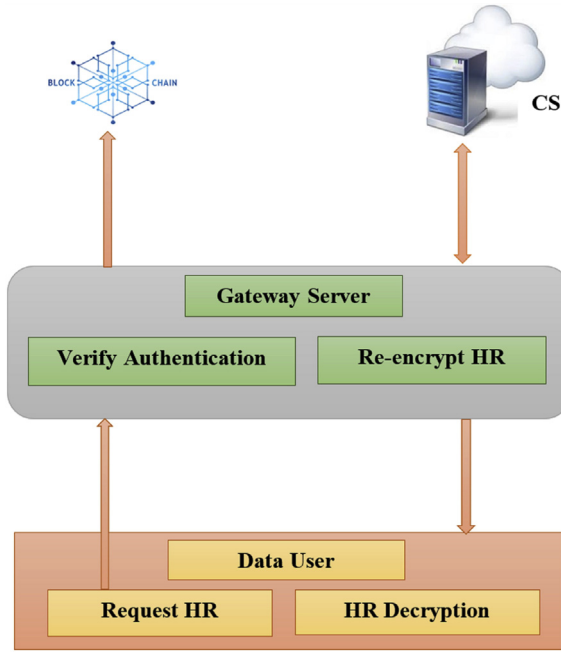

FIGURE 14.10 Downloading health record.

through the gateway service. The gateway server will validate each request under the authority of the requester according to the predefined access list provided by the owner of the HR. Once the request has been successfully verified, the gateway server will store transaction log information on the blockchain and reencrypt the HR with the corresponding reencryption key for the authorized users. As a result, by updating the ACL and retaining control of HR, the HR owner may revoke any access to his/her HR data.

If the gateway server violates the presumption that the gateway server follows the protocol (semitrusted) described in this work, it may be audited on blockchain. When a user is discovered to have an illegal activity on blockchain, the HR owner must update his/her details and encrypt the data again. This will include the encryption method for completely untrusted gateway servers.

4.10 Protocol on access control

Under the proposed model, proxy reencryption of the access control protocol reduces the gateway server requirement. As such, in the proposed model, the gateway server may be viewed as a semitrusted object. The real HR data is securely encrypted with the public key of the HR owner, and a group of

approved users can access the ciphertext according to the ACL. Updating the ACL can easily revoke the access to actual HR data. The delegated user may also add new HR data on behalf of the HR owner and create the corresponding metadata. The list of access controls is stored in the local gateway server database. The corresponding secret keys are however protected as the secret key belongs to the owner of the HR. Only the HR owner can generate the reencryption keys that are used by the gateway server. In addition, the reencryption keys only allow the gateway server to reencrypt the original ciphertext for the authorized user. Consequently, the gateway server cannot access the actual HR data, because the actual PHR data can never be decrypted on the gateway server.

4.11 Security analysis

In every model, there are five key security criteria need to be addressed by model architects, data confidentiality, data integrity, data authentication, user authentication and data availability. Data confidentiality guarantees that data are detained under the policies of access control and it should be accessed by authorized users.

Integrity of data is highly achieved using robust cryptographic protection. Integrity is responsible for nonchangeable messages sent to the destination. Data authentication is a process of verification services that provides the permission to access the protected data and data availability enables that the different kinds of information should be available and accessed at all time when they are necessary. The features of cloud data storage are low cost, consistency, high performance, availability and durability. This model can be evaluated under various threats. The adversary in this model can be a home device or any other node in the server network or providers become an attractive target for data breach. These adversaries may remove transactions, sniff messages, generate false transactions, or alter or remove information from the storage.

The security of the model is evaluated by different attacks which could be possible with this model Table 14.2. For that, this model considers some assumptions that the cyclic group generator x is not computed from (x, x^a) with undeniable probability. Next, the gateway server and CS are semitrusted, they have the curiosity to understand the data. A successful cryptosystem can withstand known attacks of all kinds which can be addressed in the following.

Theorem 1. Adversary hack the channels of public contact and get confidential information, such as medical data. The proposed RHM system is secure against the tampering of medical data by adversary.

Proof:

The medical data is encrypted and stored in the CS. The link for the storage block is only known to the gateway server. The adversary has no chance to modify data, because the message digest in block chain can track this kind of

TABLE 14.2 Security evaluation mode.

Evaluation mode	Solution
Data confidentiality	Public key
Data integrity	Hashing
Data authentication	Public key, digital signature
User authentication	Public key
Data availability	Acceptable data transactions

actions. If an adversary enters to change the record, he has to change the hash of all previous blocks. But it is very difficult to forge the data, because block chain ensures the characteristics of immutability and tamper resistant.

Theorem 2. Assume that attack occurs when two or more parties agree to reveal some secret information, illegally. For example, a cloud server and a gateway server can combine to reveal some critical information about the data owner's data. This can affect the entire privacy and security of all of the data stored in the cloud, thus severely affecting the trust of the data owner with regards to using the cloud for data sharing and collaboration purposes.

Proof:

The ACL is stored locally in the gateway server. The ACL does not contain any information about secret keys. The gateway server therefore cannot gain access to the encrypted PHR data. Since the secret key is in the control of the HR data owner, the HR data owner can only produce the reencryption keys that are used by the gateway server. The gate way server has no idea to create the reencryption keys for an adversary.

Theorem 3. The adversary can trace the transaction details of a legal user from block chain network or penetrating the channel and retrieve the information on transit, will lead to replay the information for data theft.

Proof:

The time stamp is appended with the packed data block, and it should be verifiable by gate way server. Also, it verifies the digital signature. Initially, it verifies the time stamp, if it is incorrect, the gateway server will not send any response to the adversary (DU). Consider, if the time stamp is correct, then also the adversary cannot retrieve the encrypted data. Thus, replay attack is not possible.

Theorem 4. The adversary intercepts and update or retrieve the medical data in an unauthorized access.

Proof:

The ACL plays a vital role to protect data against unauthorized access. Based on the policies, the DU seeks the data identifier from private block

chain. If the adversary does not have the valid data identifier, then he will not be able to access data. After the verification, the gateway server sends the reencrypted data with a decryption key.

Theorem 5. The adversary forges the credentials of data owner and tries to communicate with gate way server.

Proof:

Once the system can securely communicate with the gateway server or data owner, their signatures must validate one another's identity. If the attacker impersonates a valid device and sends the credentials to the gateway server, this cannot be authenticated and the adversary can revoke access to the device that is malicious or compromised. Thus, impersonation attack is impossible in this model.

5. Efficiency of proposed model

The performance of the proposed system is analyzed based on the RHM by IoT devices, cryptographic operations, the storage of the COVID-19 data set in the cloud, the metadata storage, and the access control in the blockchain. PRE is deployed for the cryptographic operations. The estimation of store and retrieve operation on 4G/5G network is done in the blockchain model for the access control signature storage.

The dataset used is the freely available COVID-19 Open Research Dataset (CORD-19) which gives the complete information regarding of the COVID patients. The CORD-19 dataset is included with the COVID19_line_list_data.csv (358.85 KB) contains the attributes such as reporting date, summary, location, country, gender, age, symptom_onset, If_onset_approximated, hosp_visit_date, international_traveler, domestic_traveler, exposure_start, exposure_end, traveler, death, recovered, symptom, source, and link. This dataset also includes covid_19_data.csv (5.14 MB) which updates the daily level information on the number of COVID-19 affected cases across the globe. time_series_covid_19_confirmed (197.03 KB) which gives the time series data on the total confirmed cases, time_series_covid_19_death (140.7 KB) displays the time series of the total data of death and time_series_covid_19_recovery data (172.32 KB) shows the time series of the total recovered cases.

5.1 Experimental setup

The experiment of the proposed model is done by the VMware workstation with Ubuntu OS. The host system is equipped with Intel(R) Core (TM) i7-4510U CPU, 2.60 GHz, 8 GB RAM, running Windows 10. Using Eclipse IDE (oxygen), Java 1.8, Java security library, Oracle Commons Lang 3.6 (OCL), Java Pairing-Based Cryptography (JPBC) the PRES encryption algorithm is implemented. For the blockchain service testing, the Hyperledger

blockchain network is created with node.js. The blockchain network contains peer nodes. For this experiment, CORD-19 is used.

CORD-19 consists of data of varying sizes. These data with the various sizes are used for the experiment which contains 64, 128, 256, 512, 1024, 1536, 2048, 2560, 3072, and 4096 KB size. The RHM scheme must respond with variety of users, the performance analysis of the proposed system is also examined with varying number of users from a minimum of 1 to a maximum of 16 users.

The performance analysis is performed using the proxy reencryption scheme, gives sufficient data storage for the IoT devices that are used for data acquisition from the patients than the attribute-based encryption scheme. PRE is implemented using the AFGH algorithm and AES (Nechvatal, Barker, Bassham, Burr, Dworkin, Foti, and Roback, 2001). Under PRE scheme the encryption algorithm used is symmetric cipher AES. The effective access control scheme for the peer nodes in the block chain is achieved by using the symmetric key for encryption. This provides a ciphertext with the combination of encrypted data and the encrypted symmetric key. Both the encryption and decryption process use the same symmetric key.

5.2 Experimental results

The RHM experiments are done by varying the data sizes, varying number of users with the real scenario for evaluation. The encryption and decryption time for the IoT device data is performed by the PRE method 50 times by documenting the average processing time. First the performance of the encryption and decryption operations are done by sharing the varying data sizes with one user. Then the analysis is done by sharing the data sizes with 2, 4, 8, 16, and 32 users, respectively. Finally, the store and retrieve time is analyzed for the entire system.

5.2.1 Encryption and decryption for varying data sizes

The performance analysis is done by sharing the CORD-19 data sizes to one user for the cryptographic operations such as encryption and decryption. The PRE method used consists of the various phases such as key pair generation, reencryption key generation, encryption, reencryption, and decryption processes. The time taken by the key pair generation phase is 2.94 ms, the time consumed by the reencryption key generation is 17.32 ms and the time for the proxy reencryption is 17.92 ms. The ABES method consists of different phases such as owner key generation, user key, encryption and decryption. The time taken to generate owner key is 360.12 ms. The time taken to generate user key is 360.80 ms. The encryption and decryption time for varying data sizes for the proposed model is calculated. Fig. 14.11 portrays the encryption time and decryption time of PRE with varying data sizes. Fig. 14.12 shows that as the

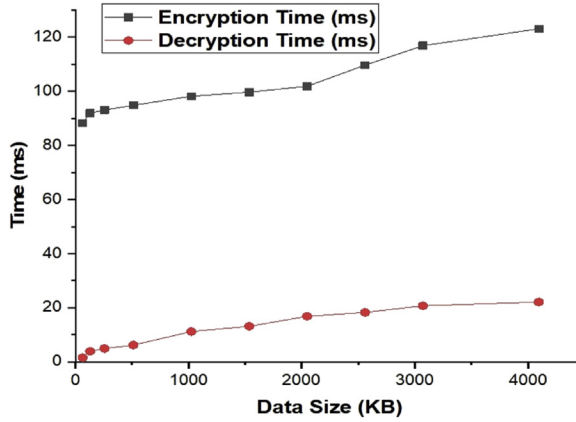

FIGURE 14.11 PRE-encryption and decryption time versus data size.

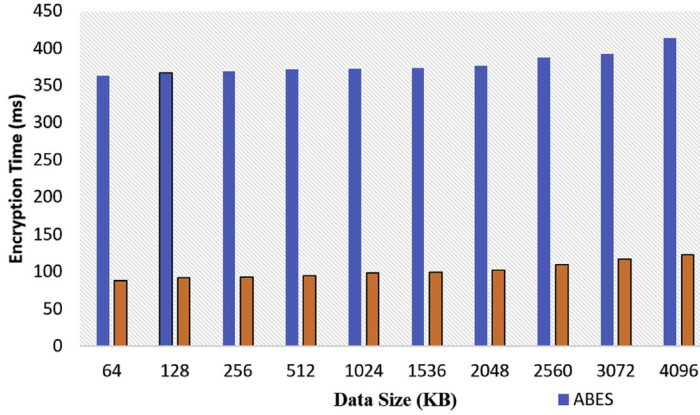

FIGURE 14.12 Encryption time for proposed and existing method.

data size increases, the encryption time gradually increased in the proposed model. Similarly, Fig. 14.13 shows the decryption time for the proposed and existing method. It is an appreciable improvement in the computation obtained from the proposed model. Based on the results presented in Fig. 14.14, the storing time and retrieving time of medical data is more efficient for better transactions. Many ABE schemes, require great computational resources for storage and retrieval of data. Given the limited capabilities of the sensors, it may not be a good idea to apply existing ABE schemes to sensors. Computational time can be calculated by summing the time of encryption and decryption as portrayed in Fig. 14.15.

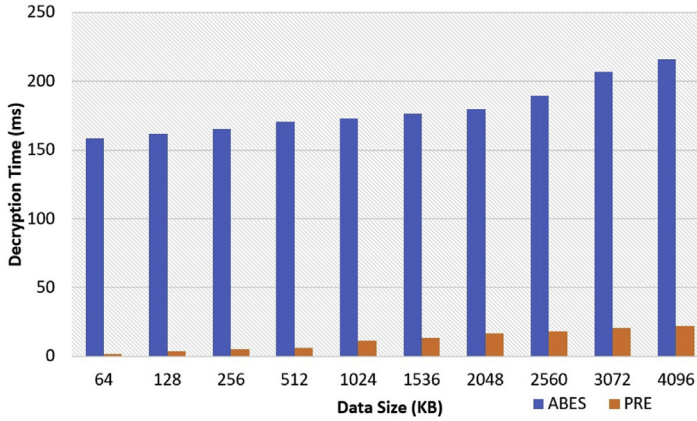

FIGURE 14.13 Decryption time for proposed and existing method.

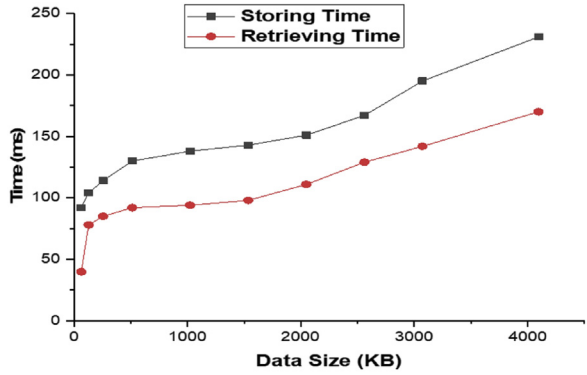

FIGURE 14.14 Storing and retrieving time for proposed method.

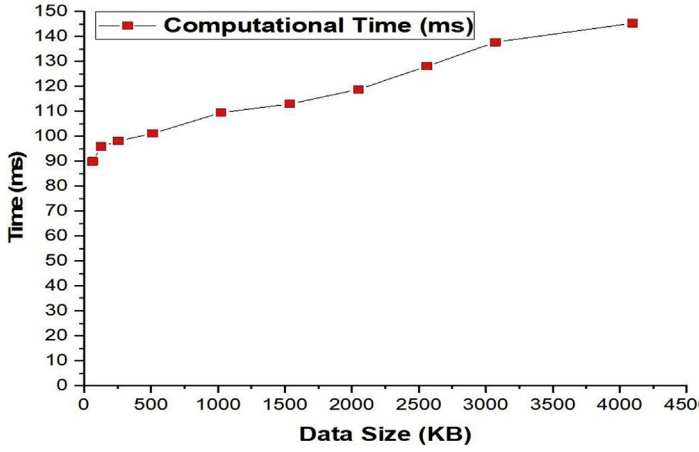

FIGURE 14.15 Computational time for proposed method.

5.3 Varying the number of users

The RHM system is used by various numbers of users and variety of data sets. The data stored in the cloud need to be shared to multiple users during the storing process and assigns different access control mechanisms in the block chain and shares as per requested in the retrieve process. These various operations are analyzed using different number of users with 4 MB CORD-19 data.

In the proposed RHM system, the proxy reencryption key is generated by the data owner for storing the HR data. As per the request, the users can retrieve the data using the proxy reencryption and the decryption process. If there is an additional authorization given by the data owner, then additional reencryption process is mandatory. Fig. 14.16 portraits that, as the number of users increase, the time taken to generate the reencryption key also increases. This is due to the time taken for the change in attribute set and policy as there is an increase in the number of authorized users. This change leads to the increase in storing operation but the retrieving operation remains with little change and is given in Fig. 14.17.

As per the results estimated, the implementation is conducted for increasing number of users such as 1, 2, 4, 8, 16, 32, and 64. Under PRE model, the storing time is increased with the varying number of users. The time taken for storing operation for 1 user is 234 ms and it is increased to 257 ms for two users. Also, it increases to 1049 ms for 64 users. The retrieval time is 71, 83, 89, 90, 93, 95, and 96 for 1, 2, 4, 8, 16, 32, and 64 users. The time taken for storing operation gets increased with the increase in number of users is due to the time taken for performing the master key generation and the encryption process. The retrieving process performs the user key generation

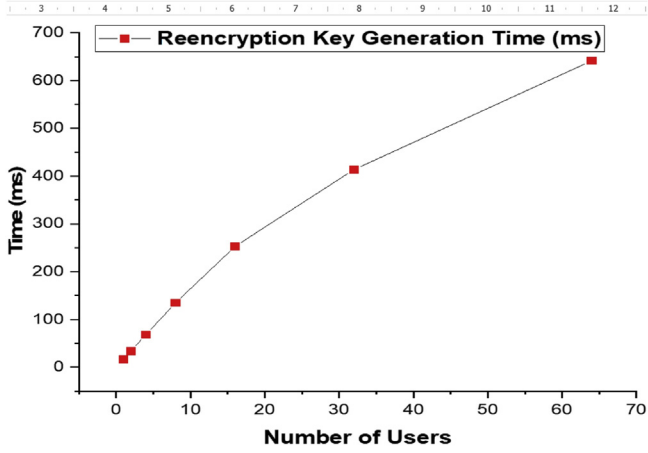

FIGURE 14.16 Reencryption key generation time.

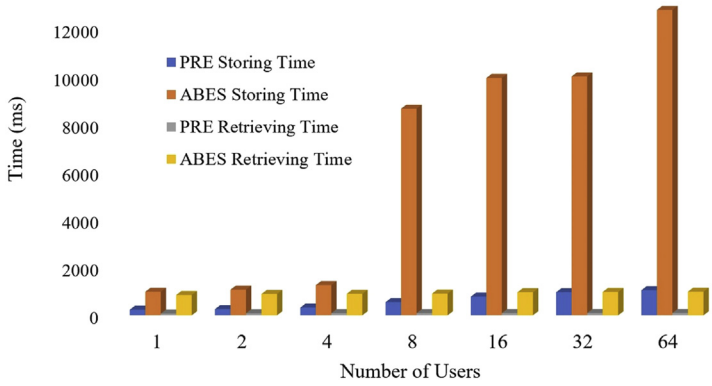

FIGURE 14.17 Storing and retrieval time versus varying number of users.

and decryption process which requires less time. The comparative results show that, there is a great difference between PRE storing time and ABES storing time. The storing time of PRE for two users are 257 ms and for ABES it takes 1073 ms. 816 ms difference obtained for both schemes shown in Fig. 14.17. The number of computational operations conducted in ABE reflects the overhead of storage and retrieval of medical data.

5.4 Throughput

Throughput can be calculated by using the number of users from 50 users to 500 users (with a time of 20−50), who use the device and perform its different functions. From the experiments, it is observed that as the number of users and requests increases, the system throughput considerably increased in a linear manner. It is increased from 118 KBps for 50 users to 865 KBps for 500 users. The linear increment of throughput indicates the efficiency of the proposed PRE model. The following Fig. 14.18 offers a summary of the proposed framework's throughput.

5.5 Latency

Latency as described earlier is the delay or time gap when one system component sends out a request and some other system component generates a response. The difference is defined as latency between those two actions. The latency is evaluated for number of users varying from 50 to 500 given in Fig. 14.19. The delay occurred for 50 users as 3.5 ms, 100 users as 5.1 ms, 150 users as 6.8 ms, and so on. The greatest delay occurred as 10.1 ms for 500 users. Fig. 14.19 offers a summary of the system's average latency.

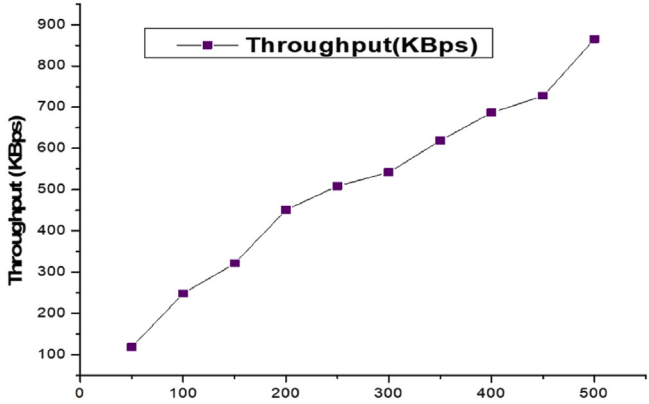

FIGURE 14.18 Throughput versus number of users.

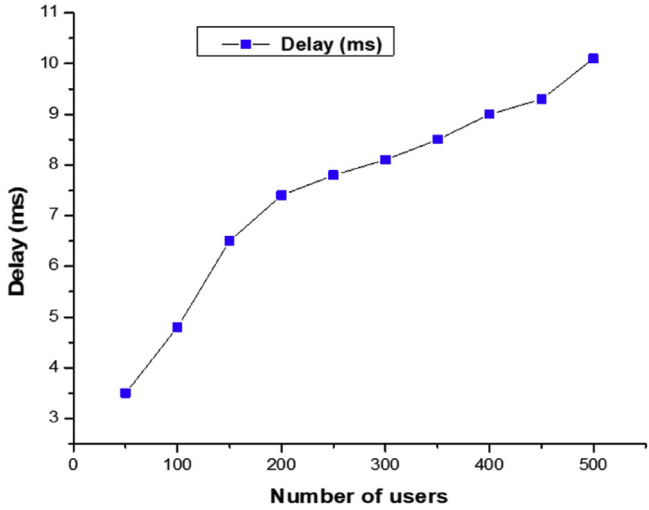

FIGURE 14.19 Number of users versus latency.

5.6 Discussion

In this experimental study, we suggested a blockchain-based access control paradigm to safeguard HR privacy. Our suggested architecture uses a proprietary database, CS and other cryptographic methods, including proxy reencryption, hashing, and digital signature to provide HR device resistance and anonymity. The proposed model can strengthen the highlights: (1) the HR owner can safely store and offer his/her HR information; (2) the HR owner can deny an entrance directly on any HR information effectively; and (3) all clients including the HR owner can advantageously check the trustworthiness of the

information. The blockchain technology is used to attain the tamper-resistance property of our platform. Consequently, problems relating to the use of blockchain in the HR system such as the usability, withdrawal of consent, and confidentiality of stored data are discussed in this research work.

The proposed model allows blockchain hold only the limited metadata to tackle the availability problem of blockchain. To maintain security, the encrypted actual HR is stored in the CS. Users can search the HR using blockchain metadata, and can order encrypted HR from the gateway server. As a result, all access to HR data should be stored on blockchain to enable an unchanging audit trail. To address the problem of blockchain secrecy, the real HR is encrypted with the HR owner's public key and only the metadata is exposed on the blockchain itself. To deal with the problem of consent revocation, the ACL, which includes the reencoding keys of the permitted users, can limit the users of a certain service. By updating the access list (revoking the reencryption key) and retaining data ownership, the HR owner can revoke access to his/her HR data.

The proposed model is evaluated from a security and performance viewpoint to ensure that the priorities are achieved. When dealing with a single individual, the theoretical model is tested on various data sizes. The model suggested outperforms when compared to the existing method for increasing data size; however, the average running time is identical for different data sizes. The existing method operational time increases explosively, while the operational time of proposed model increases linearly. The suggested solution is also not only more effective but much better suited to the HR method.

6. Conclusions

In this chapter, the blockchain-based RHM system is proposed to facilitate a privacy model that retains access control of the medical data in the COVID-19 pandemic situation. The approach suggested addresses the requirements of the HR system and the challenges of using blockchain technology in the implementation of HR systems. The protection of privacy in the HR system needs a qualitative necessity, namely the storage of tamper resistance and functional requirements, namely revocable access control. In addition, there are other concerns such as restricted storage and protection of nonchain data for the use of blockchain in HR development. Prior to IoT, patients' associations with specialists were restricted to visits, and tele and text correspondences. There were no chance to specialists or medical clinics could screen patient's well-being consistently and make suggestions in like manner. IoT empowered gadgets have made far checking in the medicinal services area conceivable, releasing the possibility to keep patients protected and solid and enabling doctors to convey standout care. Also, the proposed model expanded patient commitment and fulfillment as collaborations with specialists have become simpler and more productive. The ACL is built to be applied using existing

cryptographic techniques and private blockchain network in such a way that it can manage blockchain concerns for HR system development and determines the privacy and access control prioritization. Then the privacy and security of the proposed model is analyzed with threat models, namely a manipulative attack, a replay attack, a collusion attack, a malicious attack and an impersonation attack, to ensure that the original objectives of proposed system are met. This model is suggested not only to address HR privacy issues, but also to look forward to ongoing research into the applications of blockchain for data security and privacy protection in health care. IoT majorly reduces human services costs altogether and improves treatment results.

References

Agyekum, Xia, Q., Sifah, E. B., Gao, J., Xia, H., & Du, X. (2019). A secured proxy-based data sharing module in IoT environments using blockchain. *Sensors, 19*(5).

Ateniese, G., Fu, K., Green, M., & Hohenberger, S. (2006). Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security, 9*(1), 1−30. https://doi.org/10.1145/1127345.1127346

Atri, D., Hasan, K., Siddiqi, J., Lang, V., Nauffal, D. A., Morrow, E. A., et al. (2020). COVID-19 for the cardiologist: A current review of the virology, clinical epidemiology, cardiac and other clinical manifestations and potential therapeutic strategies. *Journal of the American College of Cardiology: Basic to Translational Science, 5*(5), 518−536.

Au, M. H., Yuen, T. H., Liu, J. K., Susilo, W., Huang, X., Xiang, Y., et al. (2017). A general framework for secure sharing of personal health records in cloud system. *Journal of Computer and System Sciences, 90*, 46−62. https://doi.org/10.1016/j.jcss.2017.03.002

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings - 2016 2nd international conference on open and big data, OBD 2016* (pp. 25−30). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/OBD.2016.11

Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In: Advances in Cryptology—EUROCRYPT '98 (Espoo). *Vol. 1403 of Lecture Notes in Computer Science* (pp. 127−144). Berlin, Germany: Springer.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform* (Vol. 3).

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310).

Chow, S. S. M., Weng, J., Yang, Y., & Deng, R. H. (2010). Efficient unidirectional proxy re-encryption. In *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 6055, pp. 316−332). https://doi.org/10.1007/978-3-642-12678-9_19

Clauson, K. A., Breeden, E. A., Cameron, D., & Mackey, T. K. (2018). *Leveraging blockchain technology to enhance supply chain management in health care: Blockchain in health care today.* https://doi.org/10.30953/bhty.v1.20

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In *AMIA Annual symposium proceedings. AMIA symposium, 2017* (pp. 650−659).

Sangeetha, D., & Vaidehi, V. (2017). A secure cloud based Personal Health Record framework for a multi owner environment. *Annals of Telecommunications*, 95−104. https://doi.org/10.1007/s12243-016-0529-4

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Health care blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*(7). https://doi.org/10.1007/s10916-018-0982-x

Gu, K., Jia, W., Wang, G., & Wen, S. (2017). Efficient and secure attribute-based signature for monotone predicates. *Acta Informatica, 54*(5), 521−541. https://doi.org/10.1007/s00236-016-0270-5

Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., & Choo, K. K. R. (2016). Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *Journal of Medical Systems, 40*(11), 235.

Haleem, A., Javaid, M., & Khan, I. H. (2020). Internet of things (IoT) applications in orthopaedics. *Journal of Clinical Orthopaedics and Trauma, 11*, S105−S106. https://doi.org/10.1016/j.jcot.2019.07.003

Ivan, D. (2016). *In moving toward a blockchain-based method for the secure storage of patient records*.

Jesus, E. F., Chicarino, V. R. L., Albuquerque, C. V. N. de, & de Rocha, A. A. A. (2018). *A survey of how to use blockchain to secure internet of things and the stalker attack*.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security and Privacy, 7*(4), 61−64. https://doi.org/10.1109/MSP.2009.87

Khan, S., & Khan, R. (2018). Multiple authorities attribute-based verification mechanism for blockchain mircogrid transactions. *Energies, 11*(5). https://doi.org/10.3390/en11051154

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Proceedings - 2016 IEEE symposium on security and privacy, SP 2016* (pp. 839−858). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SP.2016.55

Li, B., Dawei, Y., Xun, W., Lin, T., Xiaodan, Z., Nanshan, Z., et al. (2020). Chinese experts' consensus on the Internet of Things-aided diagnosis and treatment of coronavirus disease 2019 (COVID-19). *Clinical eHealth*, 7−15. https://doi.org/10.1016/j.ceh.2020.03.001

Li, W. M., Li, X. L., Wen, Q. Y., Zhang, S., & Zhang, H. (2017). Flexible CP-ABE based access control on encrypted data for mobile users in hybrid cloud system. *Journal of Computer Science and Technology, 32*(5), 974−990. https://doi.org/10.1007/s11390-017-1776-1

Liam, B., Buchanan, W. J., Jonathan, C., & Owen, L. (2018). Applications of blockchain within health care. *Blockchain in Health Care Today, 1*. https://doi.org/10.30953/bhty.v1.8

Luis, B. C. J., Frank, M. A., & Ole, L. (2018). Public health surveillance using decentralized technologies. *Blockchain in Health Care Today, 1*, 1−14. https://doi.org/10.30953/bhty.v1.17

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: a systematic mapping study. *Telematics and Informatics, 35*(8), 2337−2354.

Marek, A. C. (2018). Blockchain as a foundation for sharing health care data. *Blockchain in Health Care Today, 1*, 1−6. https://doi.org/10.30953/bhty.v1.13

Mayank, R., Danilo, G., & Katina, K. (2019). SoK of used cryptography in blockchain. *IEEE Access*, 148550−148575. https://doi.org/10.1109/access.2019.2946983

Merkle, R. C. (1989). A certified digital signature. In *Conference on the theory and application of cryptology* (pp. 218−238).

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications, 89–90*, 5–16. https://doi.org/10.1016/j.comcom.2016.03.015

Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*.

Nasir, Q., Qasse, I. A., Abu Talib, M., & Nassif, A. B. (2018). *Performance analysis of hyperledger fabric platforms*. Security and Communication Networks. https://doi.org/10.1155/2018/3976093

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J., & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). *Journal of Research of the National Institute of Standards and Technology, 106*(3), 511.

Nunez, D., Agudo, I., & Lopez, J. (2017). Proxy re-encryption: analysis of constructions and its application to secure access delegation. *Journal of Network and Computer Applications, 87*, 193–209.

Ostrovsky, R., Sahai, A., & Waters, B. (2007). Attribute-based encryption with non-monotonic access structures. In *Proceedings of the ACM conference on computer and communications security* (pp. 195–203). https://doi.org/10.1145/1315245.1315270

Radanovi, & Liki, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy, 16*, 583–590. https://doi.org/10.1007/s40258-018-0412-8 [Medline: 30022440].

Rao, Y. S. (2017). A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing. *Future Generation Computer Systems, 67*, 133–151. https://doi.org/10.1016/j.future.2016.07.019

Rifi, N., Agoulmine, N., Chendeb Taher, N., & Rachkidi, E. (2018). Blockchain technology: Is it a good candidate for securing IoT sensitive medical data? *Wireless Communications and Mobile Computing, 2018*. https://doi.org/10.1155/2018/9763937

Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., et al. (2014). Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine, 52*(8), 74–81. https://doi.org/10.1109/MCOM.2014.6871673

Tariq, N., Asim, M., Al-Obeidat, F., Farooqi, M. Z., Baker, T., & Hammoudeh, M. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors, 19*(8).

Wang, D., Hu, B., Hu, C., Zhu, F., Liu, X., Zhang, J., et al. (2020). Clinical characteristics of 138 hospitalized patients with 2019 novel coronavirus-infected pneumonia in Wuhan, China. *JAMA - Journal of the American Medical Association, 323*(11), 1061–1069. https://doi.org/10.1001/jama.2020.1585

Wang, Y., Hu, M., Li, Q., Zhang, X. P., Zhai, G., & Yao, N. (2020). *Abnormal respiratory patterns classifier may contribute to large-scale screening of people infected with COVID-19 in an accurate and unobtrusive manner.*

Wangthammang, M., & Vasupongayya, S. (2016). Distributed storage design for encrypted personal health record data. In *2016 8th international conference on knowledge and smart technology, KST 2016* (pp. 184–189). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/KST.2016.7440505

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less medical data sharing among cloud service providers via blockchain. *IEEE Access, 5*, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings - 2017 IEEE 6th international congress on big data, BigData congress 2017* (pp. 557–564). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BigDataCongress.2017.85