Journal of Ambient Intelligence and Humanized Computing (2020) 11:4613–4641
https://doi.org/10.1007/s12652-020-01710-y

ORIGINAL RESEARCH

MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption

Seyed Morteza Pournaghi[1] · Majid Bayat[2] · Yaghoub Farjami[1]

Received: 24 July 2019 / Accepted: 7 January 2020 / Published online: 21 January 2020

Abstract
The development of Electronic Information Technology has made the Electronic Medical Record a commonly used approach to recording and categorizing medical patient data in databases of different hospitals and medical entities so that controlling the shared data is not possible for patients at all. The importance of medical data as possessions of people and the system leads us to be concerned about its security, privacy, and accessibility. How to store and controlling access to medical information is of the most important challenges in the electronic health area. The present paper provides a new, secure, and efficient scheme based on blockchain technology and attribute-based encryption entitled "MedSBA" to record and store medical data, indicating that our proposed scheme protects user privacy and allows fine-grain access control of medical patient data based on General Data Protection Regulation (GDPR). Private blockchains are used in MedSBA to improve the right to revoke instant access which is of the attribute-based encryption challenges. The security and functionality of our proposed scheme are proved within a formal model and based on BAN logic, respectively; simulating the MedSBA scheme in the OPNET software as well as examining its computational complexity and storage indicates the efficiency of the present scheme.

Keywords e-Health · Blockchain technology · Attribute-based encryption · Security · BAN logic · OPNET

1 Introduction

The provision of health services via using digital technology is called "Electronic Health". The World Health Organization (WHO) defines Electronic Health in 2005 as follows: "Applying digital data to the health-care field is called Electronic Health used to store and retrieve data within a network to support health care at a local and large scale". Improving communication between health care providers will help a lot in avoiding unnecessary and duplicate trials, diagnosis, and treatment and reducing medical costs. By increasing the effect and possibility of exchanging information between health centers and joint decision-making for treatment, electronic health leads to an increase in health care quality. Health care systems collect comprehensive physiological information and medical records, increasing the importance of medical data. Such a comprehensive database makes it possible to discover useful information and environmental factors required for identifying rare disorders and medical treatments (Wu and Tsai 2018).

Electronic Health Record is an electronic medical record including all information related to the health of a person during his or her life. Having proper structure and standards and preserving the confidential principles, a health electronic record provides a lifelong file including an individual's health history and medical care in the health system. Electronic health records include health-care records of an individual's lifetime, such as medical pictures, medical treatments, medications, empirical reports, family medical history, genetic diseases, etc. that keeping confidentiality are stored privately within the healthcare system. This file should be electronically available to the authorized medical providers at any location and time to support the improvement of the quality of services. Therefore, Electronic Health Record as a secure and expandable electronic information system is available to the users of health care centers authorized to access the data history of patients to add new

✉ Yaghoub Farjami
farjami@qom.ac.ir

Seyed Morteza Pournaghi
sm.pournaghi@stu.qom.ac.ir

[1] Department of Computer Engineering, University of Qom, Qom, Iran

[2] Department of Computer Engineering, Shahed University, Tehran, Iran

treatment information at any time. Hence, using EMR helps a lot in preventing diseases and improving the treatment process of a patient (Cartwright Smith et al. 2016; Kshetri 2017; Hamza et al. 2019).

Sharing the secure and scalable Electronic Medical Record (EMR) is essential for more effective treatment management, the cooperation of medical entities, and the acceleration of the care and treatment process of patients. Individuals often visit doctors in hospitals and health care centers during their lives and submit a variety of medical information at each visit. Health centers should be able to confidentially and promptly update and share the medical patient information with other authorized entities to provide effective, accurate, swift and affordable health care services. Providing adequate medical information, immediate and secure data sharing avoids planning errors in the patient-treatment process so that medical specialists can improve the accuracy of treatment-processes and recognize the needs of patients to apply more effective treatment.

Many medical institutions have recently commenced collecting EMR data from patients with a variety of mechanisms; however, this approach lacks medical data sharing. Consequently, some centralized models for EMR data collection have been developed to improve the usability and sharing of EMR data, as well as the convenience of patients and treatment centers. Since creating centralized EMR data models requires costly and complex technical support, the cloud-based storage system can be considered an appropriate alternative. The advantages of applying cloud-based storage technology include fast data transmission, better data sharing, high storage capacity, low cost, easy access to information and dynamic communication. A cloud-based storage system can be used as an appropriate platform to share EMR information between different hospitals and patients to support the development of intelligent medical services and data storage. However, when users store EMR data on cloud servers, they encounter a variety of security threats such as data integrity, authentication, and privacy violations. So there are a lot of risks to the centralized management of medical data. Medical data can easily be stolen, manipulated, or even totally removed. In such cases, medical data cannot be reliably recorded or retrieved, which may delay the treatment process or even endanger the life or safety of patients (Azaria et al. 2016).

Nowadays, medical information is more important than the credit card password. Any damaging attack to a system in the centralized systems will destroy all other nodes making it impossible to store and use data. Despite any destructive attack to some nodes, applying the technology of blockchain distributed architecture makes the network continue to exist with no more effect on other nodes. Security professionals and scholars are not sure to store important medical information in the centralized database; most people are also still worried about the security and privacy of such databases. One of the concerns in this area is how to apply access control policy to medical information. It is required network members as a whole trust in a centralized entity that evaluates access control policies to implementing the requested access to a data source. In this architecture, it is possible for the central entity to ignore some data access policies and act contrary to the expected procedure of the network (Dagher et al. 2018).

Having been discussed in recent studies, a promising technology called blockchain addresses decentralization objectives and smart contracts. Blockchain can thus access the Internet of Things for more applications such as smart medicine where patients, using blockchain technology, can securely and preserving privacy access their medical records. There are many barriers to medical data sharing in the technical infrastructures of the Health IT systems, avoiding secure and scalable access to medical data throughout the network. The concerns include patient privacy-preserving, lack of confidence between health entities, scalability, and control of the right to access information accurately (Yue et al. 2016).

Blockchain-based technologies as technical infrastructures have recently been promoted to support clinical data sharing to improve medical services. Blockchain having the feature of "trust with no intermediaries" enables multiple parties who do not fully trust each other to exchange their digital resources together and preserve their vital and personal information, as well (Banerjee et al. 2018). In this paper, an approach based on blockchain technology is proposed to provide the right to access a data source and allow the transfer of such rights among users.

1.1 Our contributions

Providing an architecture for sharing and storing medical data by integrating attribute-based encryption and blockchain technology: We introduce a novel architecture along with its implementation in detail for sharing secure and scalable medical data to preserve user privacy. In this paper, we propose a secure and efficient method to control access to register and store medical data combined with attribute-based encryption, blockchain-based protocols, and cloud storage systems to solve the security problems related to effectively sharing medical information and providing fine-grain access to medical information that also preserves user privacy. The MedSBA scheme using the attribute-based encryption attempts to preserve patient-privacy and control the fine-grain access to medical data. We have presented an architecture based on smart contracts and two private blockchains "permission and permissionless" to ensure medical data accuracy with no change and effective authentication of the users, and to improve the revocation and approval of

the right to access medical data as an important challenge in the attribute-based encryption.

Store a large amount of encrypted medical data in the cloud servers on random paths: A large amount of medical data is preserved in cloud storage systems to increase system efficiency. Because of the inefficiency of public key encryption methods for encrypting data in large scale, we use symmetric cryptography to preserve the confidentiality of medical data; however, the key is encrypted by the attribute-based encryption algorithms. We use two attribute-based encryption structures including the KP-ABE structure used to control the access level of health and service providers such as hospitals, laboratories, insurance companies, and the CP-ABE structure used for individuals and wards where patients tend to provide their medical information, according to their access policy.

Using attribute-based encryption to encrypting symmetric encryption key and storing it in private blockchain: Given that the PHR can include EMR information, medical records such as test results and radiology and MRI images, etc., storing such a large amount of medical information for every single one is not optimal in blockchain; hence, using symmetric encryption key in this method, the PHR information is encrypted and randomly stored in distributed cloud systems, encryption symmetric key and the file storage path are then encrypted using attribute-based encryption based on appropriate access structure then stored in blockchain along with the access policy and authorized conditions required for information decryption.

Using smart contracts and public and private blockchain for easy and secure access to medical data: Private blockchain used in this system makes blockchain information invisible to all. The medical data consumer entities apply smart contracts to provide a transaction based on data using authorization with a specific access structure, in case of confirming which in the blockchain network, the transaction where data storage path and its encryption key are encrypted will be available to the entity.

Formal security analysis and simulations: We evaluate the accuracy of the functionality of our proposed protocol based on BAN logic, proving that it can meet the security requirements of medical data sharing. Moreover, we prove the attribute-based encryption protocols used in this architecture are secure in a formal method and random oracle model; we present a simulation of the computation cost and storage space of our proposed scheme in OPNET to prove the effectiveness of MedSBA scheme.

1.2 Advantages of proposed scheme

Increasing flexibility and scalability: In our proposed scheme, considering that medical data is not stored in the blockchain and permission and permissionless blockchains are used to access medical information encryption keys, medical information exchange is prepared in a lightweight form.

Because only a brief description of the medical data in the permissionless blockchain and the abstract of the medical information along with its storage path in the cloud is stored in the permissioned blockchain; therefore, if the size of medical data is N, the medical description size ε_1, and its storage path in the cloud ε_2, then the complexity of total amount of information stored in the total network blockchains will be equal to $O(hash(N) + \varepsilon_1 + \varepsilon_2)$. Given that the output of the Hash function is always constant, so the space consumed in blockchain remains constant, too. The amounts of the data abstract and the reference pointer can be significantly lower than the actual size of the data. Therefore, in this scheme, using a constant-sized description, we have increased the scalability instead of using real data.

Fine-grain access control: To achieve fine-grained access control property, permissions to access a data source can be given or revoked by providers from different institutions regardless of their trust relationships. Applying CP-ABE and KP-ABE cryptography based on an appropriate access structure desired to the medical data producers in the MedSBA scheme makes fine-grain access control on the medical data possible for the user.

Instant revocation of the right to access: One of the challenges ABE encryption has always been facing is instant revocation of the right to access data. In the MedSBA scheme, in addition to having the appropriate attributes in data access structure, given the need to refer to the ITx transaction registered in the blockchain, which is an access license to medical data, the possibility of immediate revocation of the right to access information is easily provided by the medical data producers. Registering a transaction of canceling the right to access in blockchain, the source of the data producer can immediately revoke permission to access a specific entity without altering other prior rights and any trouble.

Security: Medical data in MedSBA is encrypted by the AES algorithm and its encryption key by the ABE algorithm based on the preferred attributes, and the nodes of the blockchain network directly monitor accessing the key information and encrypted data; hence, only the entities authorized by the nodes of the blockchain network can access medical data. Even if the blockchain network is threated by a 51% attack the information of the key and the data storage location in the cloud will be revealed, since data encryption key is encrypted by the appropriate attributes in ABE encryption, being unable to solve the hard problem of DMBDH or DBDH the attacker cannot access medical information at all.

1.3 Paper organization

Section 2 reviews the previous work in the medical data sharing field. Section 3 states the requirements for the proposed scheme. Section 4 presents the proposed architecture along with the details of protocols. Section 5 analyzes the security and Sect. 6 analyzes the functionality and simulation of the proposal. In the end, Sect. 7 provides concluding and future work.

2 Related work

Cloud-based storage systems have entered into e-Health systems to store medical data. These methods offer promising solutions for sharing PHI data among medical institutions in e-Health systems, where security and privacy-preserving are of critical concerns. Riad et al. (2019) proposed a new access control mechanism (SE-AC) for cloud-based IoT health-care systems. Their scheme incorporates the Attribute-Based Access Control (ABAC) technique and storage in cloud systems. Their proposed mechanism empowers the patients to control their own EHRs data and set self-policies.

All the above measures are located in the cloud environments to obtain security attributes; however, there is still a challenge in all methods. Hence, there are always concerns about misusing medical data, loss, leakage or stealing of PHI information. Many actions have been proposed using cryptography or other methods but, unfortunately, such threats have always remained given the attributes of centralization of the cloud environments. Preserving a list of distributable and unchangeable files, blockchain presents a new approach to address the security challenges inherent in cloud-based systems. Hence, nowadays, developing blockchain-based medical systems is considered an increasing matter (Kaur et al. 2018).

Yue et al. (2016) have presented an application for sharing health care data, using which patients can easily control and send their data. The scheme includes a three-layer system, data usage layer, data management layer, and data storage layer. There is a difference between this scheme and the other ones due to using blockchain as the cloud. Xia et al. (2017b) have proposed the MeDShare system in which medical data sharing among the large medical data servers, is reviewed in an unreliable environment. According to a permissioned blockchain in this system, only the invited and verified entities are authorized to access the blockchain. Azaria et al. (2016) have presented the MedRec system, a decentralized record management system based on blockchain for e-health history. The permissioned blockchain used in this platform for managing authentication and data sharing is only accessible to the authorized users. In this system, miner nodes are encouraged to participate in mining by accessing medical metadata.

Peterson et al. (2016) have offered a healthcare system based on blockchain integrated with FHIR standard considerations. They proposed a Merkle-tree based blockchain system that represents "Proof of Interoperability" as the consensus system for block mining. Proof of interoperability in this system is in conformance with the FHIR protocol, that is, miners must verify the clinical messages sent to their blockchains to make sure they are interoperable with identified structural and semantic standards. Dubovitskaya et al. (2017) have proposed a permissioned blockchain framework for managing and sharing medical documents to care for cancer patients. Membership service is applied to their scheme to authenticate and verify registration of user membership service through using a username/password. Personal ID information (social security number, birthday, name, and zip code) is necessary for generating patient identity and security encryption. Access to medical data files uploaded to the cloud server is managed using blockchain logic. The proposed scheme Karafiloski and Mishev (2017) applies smart contracts containing the metadata on assets history, permissions, and data integrity. The state functions of contracts in this scheme are transferred based on the policies set in the legal transactions.

Since such studies have used the blockchain just as a storage device, the likelihood of sharing the cooperative medical data using fine-grain access control by the related producer entity is not explained well in the aforesaid schemes. Moreover, these schemes provide no exact solution along with the details on its required protocols. Hence, this paper presents a fine-grain access control method based on ABE and blockchain for storage and access to medical data as well as details of this scheme.

Most recent methods in e-health data sharing regularly collect high-resolution personal data of which the user has no specific knowledge or control about them. Furthermore, people's medical information is very important and should not be aggregated to an entity. Also, PHRs and EMRs are stored in different hospital's databases, even for the same patient. Consequently, it is difficult to construct a summarized EMR for one patient from multiple hospital databases due to security and privacy concerns. To solve the above issues in e-health data sharing, we propose the MedSBA scheme which uses attribute-based encryption for fine-grain access control under different policies. Moreover, in this scheme, we use a private and public blockchain to distribute the access level on the network so that an entity could not breach security features alone. Furthermore, we improve the immediate revocation process of the user's attributes, which is one of the primary challenges of attribute-based encryption (Fernndez-Alemn et al. 2013).

3 Preliminaries

This section includes the requirements used in the MedSBA scheme such as introducing the ABE encryption, the structure and different consensus methods of blockchain, and smart contracts.

3.1 Elliptic curve group

Suppose the E/F_p symbol represents the E elliptic curve over the prime finite field F_p, while P is a large prime number, the elliptic curve E is defined as follows (Vahedi et al. 2017):

$$E : y^2 = x^3 + ax + b$$

Where $a, b \in F_p$ and $\Delta = 4a^3 + 27b^2 \neq 0$. The points on E/F_p and the infinity of O construct a cyclic additive elliptic curve group.

$$G = \{(x, y) : x, y \in F_p, E(x, y) = 0\} \cup \{O\}.$$

For further details on elliptical curves, refer to reference (Hankerson et al. 2004).

3.2 Bilinear pairing

Assume that G_1 is a cyclic additive group of an elliptic curve with generator P, and G_2 is a multiplicative cyclic group of order prime p with generator g. The mapping $e : G_1 \times G_1 \longrightarrow G_2$ is a bilinear mapping if the following requirements hold (Boneh and Franklin 2001; Kshetri 2017).

- Bilinearity: for all $X, Y \in G_1$ and $a, b \in Z_p^*$, we have $e(aX, bY) = e(X, Y)^{ab}$.
- Non-degeneracy: For all $X \in G_1$ and $(X \neq 0)$, there is a single $Y \in G_1$ such that $e(X, Y) \neq 1$.
- Computationality: For all $X, Y \in G_1$, there is an efficient algorithm to find mapping $e(X, Y)$.

3.3 The difficult problems of an elliptic curve and bilinear pairing

Elliptic curve discrete logarithm problem (ECDLP): Given an elliptic curve E defined over a finite field F_p, a point $P \in E(F_p)$ of order n, and a point $Q \in (P)$, find the integer $l \in [0,\ n-1]$ such that $Q = l.P$. The integer l is called discrete logarithm of Q to base P, denoted $l = log_p Q$.

Decisional bilinear Diffie–Hellman (DBDH): Suppose a challenger chooses $a, b, c, z \in Z_p$ at random. The Decisional BDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ with more than a negligible advantage.

Decisional modified bilinear Diffie–Hellman (DMBDH): Suppose a challenger chooses $a, b, c, z \in Z_p$ at random. The Decisional MBDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{ab/c})$ from $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ with more than a negligible advantage.

3.4 Lagrange interpolation

Interpolation is a method of finding a function value within the range of a discrete set of known data points. Lagrange interpolation is a known method to interpolate polynomials (Berrut and Trefethen 2004). Suppose the value of the function f is given in $x_0, x_1, ..., x_n$, $n+1$ distinct points, then there is a unique polynomial $P(x)$ with a maximum degree of n:

$$P(x_k) = f(x_k), \quad k = 0, 1, ..., n \tag{1}$$

The polynomial $P(x)$ is calculated as follows:

$$P(x) = \sum_{j=0}^{N} L_i(x) f(x_i), L_i(x) = \prod_{j=0, j\neq n}^{n} \frac{x - x_j}{x_i - x_j} \tag{2}$$

The symbol of $\triangle_{i,s}(x)$ represents the polynomial of the Lagrange Coefficients, computed as follows:

$$\triangle_{i,s}(x) = \prod_{j\in s, j\neq i} \frac{x - j}{i - j} \tag{3}$$

3.5 Attribute-based encryption

Attribute-based encryption is a kind of public key encryption that applies user attributes as a public key. User identification is as a specific attribute, so the attribute-based encryption can implicitly include identity-based encryption as well (Shamir 1984; Boneh and Franklin 2003). Key policy (KP-ABE) and cipher policy (CP-ABE) are two different attribute-based encryptions. Cipher-text in KP-ABE encryption depends on a set of attributes and user private-key is dependent on an access structure. In this method, the user decrypts the cipher-text only when the attribute set satisfies the access structure. Hence, the user's private key is associated with the access structure to control what cipher-texts the user can decrypt (Sahai and Waters 2005; Goyal et al. 2006).

In the CP-ABE encryption, unlike KP-ABE, the user private-key is dependent on the number of arbitrary attributes, and the encoder encrypts a message adopting a specific access policy. A user in this method can decrypt a cipher-text if and only if the attributes of the user meet the policy

determined by the cipher-text. Therefore, the cipher-text in CP-ABE is associated with the access structure to control which user can decrypt the cipher-text. Accordingly, the cipher-text is labeled in KP-ABE and if the user key access structure matches the labels the user can decrypt the cipher-text. But in CP-ABE, the user private-key is labeled, and the cipher-text has an access structure; and if the set of private-key labels satisfies the very access structure, it can access the ciphertext. In short, it is demonstrated in KP-ABE to what messages a user can access, while in CP-ABE is indicated which user can read a cipher-text. Figure 1 shows these processes.

Moreover, we require an ABE scheme in MedSBA that we can use both CP-ABE and KP-ABE. Thus, in our scheme, we assume that the universe of attributes can be partitioned into m disjoint sets. The primary challenge in creating ABE is to prevent collusion attacks between users that obtain key components from different authorities. Also, the ABE scheme used in MedSBA must be collision-resistant to maintain the required security features, and must additionally be efficient to have proper performance in the medical data sharing process (Zheng 2011; Zhong et al. 2018).

3.6 Blockchain

Blockchain is regularly considered a set of techniques used in decentralized networks to preserve a coordinated database among all the members. Satoshi Nakamoto was the first one who introduced this method for creating some techniques to establish cryptocurrency such as Bitcoin (Nakamoto 2019). The difference between blockchain structures with a centralized traditional network structure is that there are no fixed central nodes in these networks, and having relatively similar positions, all members in the network store a copy of the blockchain information. Indeed, blockchain is an immutable distributed ledger based on the time used to share and store data in a distributed form. Saved data may include payment information (such as Bitcoin and Litecoin), contracts (such as Ethereum), or personal and medical information. Therefore, blockchain is a distributed database that generates an ordered list of stored and associated information through a chain in the blocks. A block usually contains the previous hash block, data content, the participant signature, and the timestamp. The previous hash block causes the information in blockchain to remain immutable.

The main reason why blockchains do not need a centralized database to store any transaction is that blockchain technology introduced as a distributed model can store interactions through a peer-to-peer system as well as the details of each transaction in a node. Blockchain makes it possible to add new data to transactions; however, it allows no change in them. Transactions are signed by the user private-key to ensure that the data source is authenticated and not denied, and then the hashing process is added to verify the integrity of the transaction and confirm that it is unchangeable. Transactions are in the form of specific blocks and available to all network nodes to make network interactions visible to all network members. Users can generate an arbitrary number of public keys, which can effectively avoid any tracking and guarantee user's privacy (Kosba et al. 2016).

3.6.1 Blockchain functionality

To use blockchain, you first need to create a P2P network with all the nodes interested in using blockchain. Each network node generates two keys; a public key used by other

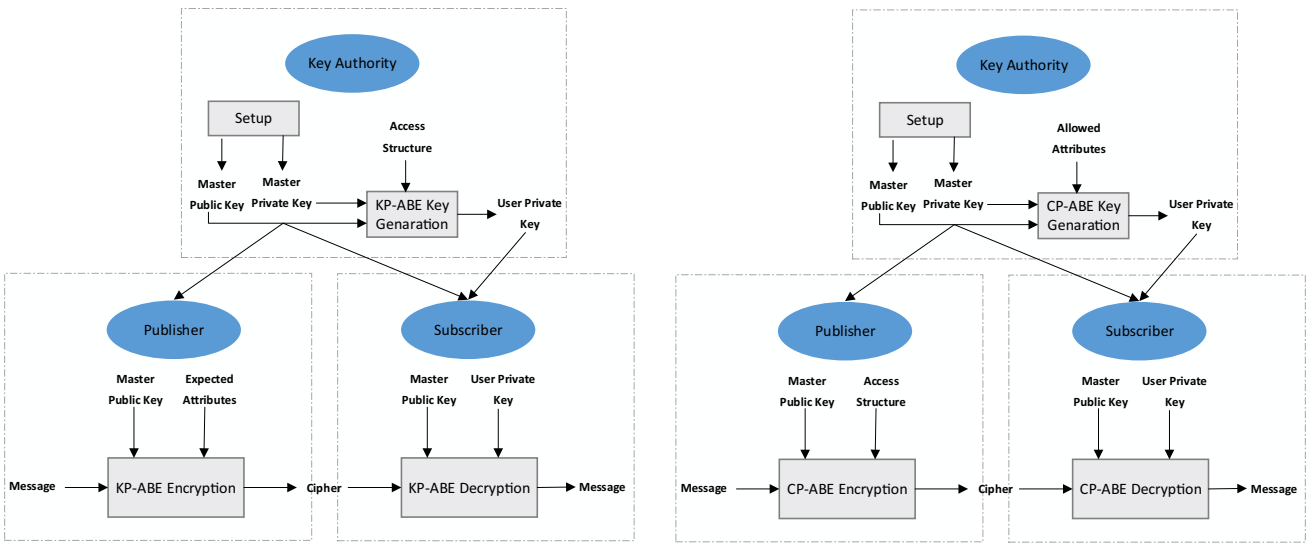

Fig. 1 How to encrypt KP-ABE and CP-ABE

users to send messages to the node; and a private key used to sign the messages sent by the node. A node after performing and signing a transaction, distributes it to its counterparts. Using a digital signature in each transaction with a unique method (using a private key) allows its authentication (only the user can sign it using a particular private key) and ensures integrity (in case any error occurs while transferring data, the transaction will not be verified). The peer node will replay a received transaction on the network after confirming its validation; hence, this approach is effective in broadcasting proper messages. The specific nodes called " Miner" verify and group the distributed transactions into blocks according to their release time on a network. How to select miners and data existing in a block depends on the consensus algorithm used in the blockchain. The grouped blocks are replayed on the network by the miners. The nodes of a blockchain network then verify the authenticity of the distributed block including all transactions in the block and the appropriate reference of the block to the previous hash block distributed on the network. The nodes will add the block to their chain and update their blockchain if both conditions are successfully approved, if not, the nodes will delete the block (Fig. 2).

Consensus algorithm as the heart of a blockchain may have different methods depending on the blockchain applying to different domains. The consensus algorithms in a blockchain can be generally grouped based on the right to access the blockchain information (such as permissioned and permissionless) as well as the right to mine their blocks (such as public and private blockchain). Without being confirmed by the third entity, each node can join a public blockchain and act as a simple or miner/validator on the network.

A group of nodes in private blockchains determine or limit the ownership of the right to access the network. The users authorized to transact and the nodes enabled to implement smart contracts or activate as miners are determined and controlled in many private blockchains, conserving all the private blockchains are not necessarily permissioned. For instance, an organization can use a private blockchain based on Ethereum that is not a permissioned blockchain. Some samples of permissioned blockchains are those used by HyperledgerFabric (Cachin 2016) and Ripple (Schwartz et al. 2014).

Consensus algorithm in both public and permissionless (such as Bitcoin and Ethereum) and private and permissioned blockchains (such as Hyperledger) is necessary for choosing and determining miners to produce and register new blocks in the blockchain. Applying the consensus method is common in the public blockchains PoW, PoS and DPoS, and the private blockchains PBFT and RAFT. Our proposed scheme applies two permissionless and permissioned private blockchains. In these blockchains, trusted participating nodes are selected to realize the mechanism of the PBFT-based consensus process. Applying the private blockchains has more control over the privacy of users, and this is an important attribute that we need in medical records and patients are always concerned about it.

3.6.2 PBFT-based consensus method

The PBFT algorithm (Sukhwani et al. 2017) is based on the Byzantine Generals Problem (Castro et al. 1999) and attempts to achieve a global agreement on the network assuming that the system error occurs by repeating the voting layers. Lamport et al. (1982) examined the probability of reaching this agreement on the assumption of error, and they proved that the expected agreement having the nodes with more than 1/3 was impossible. The BPFT consensus method can only resist the Byzantine error if at least 2/3 of the network nodes are honest. So given n represents the whole consensus nodes and f denotes all Compromised and destructive nodes, then there will be a successful consensus if $n \geq 3f + 1$. This section summarizes the PBFT consensus method used in the MedSBA system. PBFT consensus method in MedSBA includes 5 phases as follows (Fig. 3):

- Generate block: A leader is responsible for creating a new candidate block. In our system, the consensus nodes produce a new candidate block, in turn. That is, each consensus node turns into a leader in sequence.

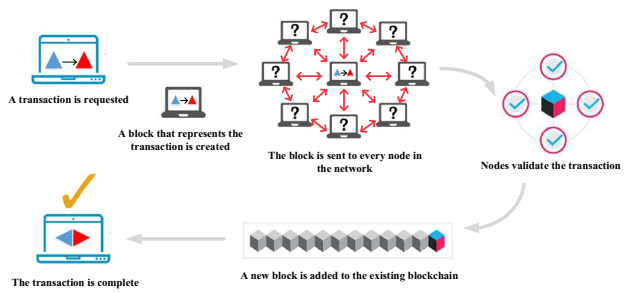

Fig. 2 Blockchain structure

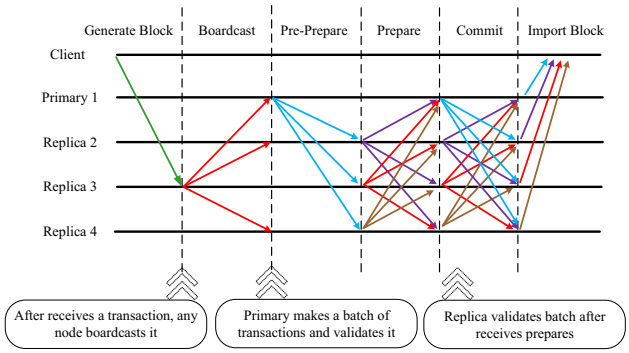

Fig. 3 PBFT consensus method

- Pre-prepare (block data): Leader node broadcasts the candidate block to other consensus nodes.
- Prepare (block hash): Every node that receives a block validates the record and broadcasts a prepare message along with the hash block.
- Commit (block hash): After receiving a sufficient number of prepare messages (for instance, the total number of messages to be more than two-thirds of the whole nodes), the commit message is calculated for each message and broadcasted to all nodes.
- Import block: If the number of the commit messages is more than two-thirds of the total number, nodes will reach a consensus on the proposed block.

3.6.3 Smart contracts

Szabo (1996) produced Smart Contracts in 1994, as a protocol executing a computer transaction contract. When a smart contract integrates to a blockchain, it stays forever. Any smart contract can be part of a database with a unique address; distributing a transaction to its address can enable its functions to manage the very part of the database. The concept of a smart contract refers to a set of software codes specifying the conditions for its predetermined implementation. Smart contracts are often organized into the "if ... then ..." conditional form. Smart contracts allow codes to autonomously execute, without human intermediation and the third party observation in case of meeting the conditions. The smart contractor sets it in a blockchain. Users then enable it by sending the required parameters to the address of the smart contract. In the MedSBA scheme, the smart contract receives a registered transaction in the blockchain as an input, and after verifying the terms of the contract on the output, restores in the cloud a transaction proportional to the encryption key and its storage location path.

4 The proposed scheme

This section describes how the MedSBA proposed scheme is used to store and share PHI medical data and how to implement each stage of the scheme, as well. There are three phases in the MedSBA scheme, producing medical content, storing, and using PHI information. These processes are shown in Figs. 4, 5 and 6 . The attribute-based encryption integrated to the blockchain technology has been used to register and store medical data making the privacy of patients preserved; providing PHR data sharing for different entities, allowing patients to have fine-grain access to control and confirm medical information with high confidence. This system has applied two private blockchains: the permissioned private blockchain is used to store the information of encryption key and the storage path for PHI data in the cloud to which the entities using medical data have access; the permissionless private blockchain is used to store PHI data brief description and the keywords associated with the data stored in the permissioned private blockchain, which is accessible for all medical entities and hospitals.

Both blockchains have different natures and functions; however, hospital computers and patients can jointly

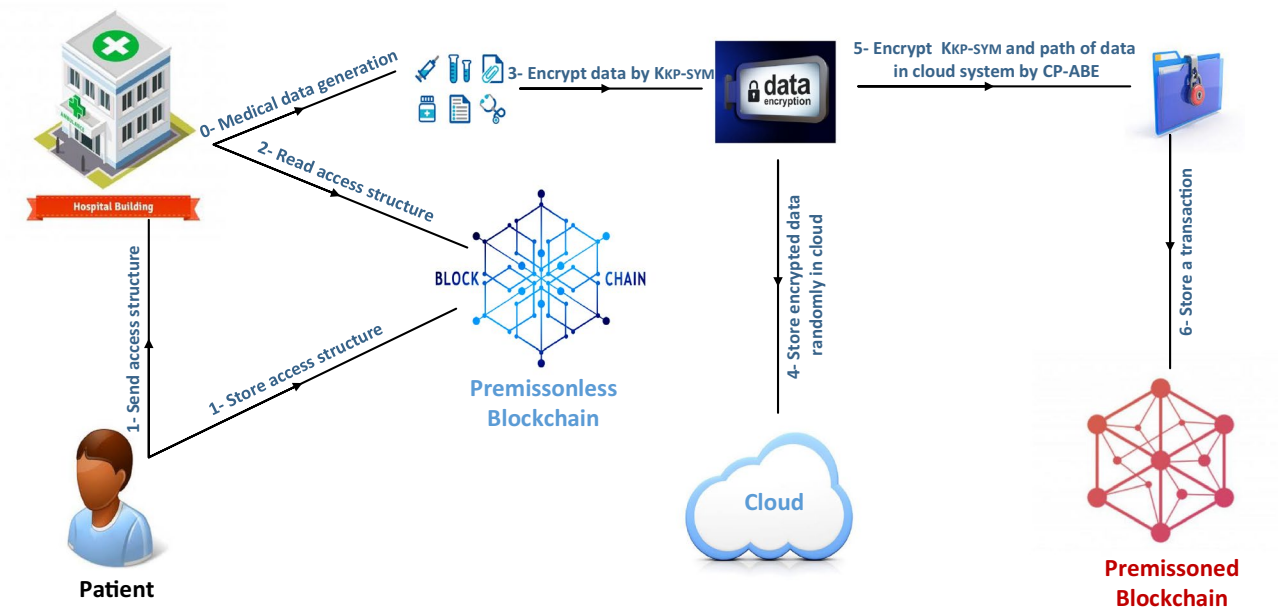

Fig. 4 How to register medical information by a hospital in MedSBA scheme

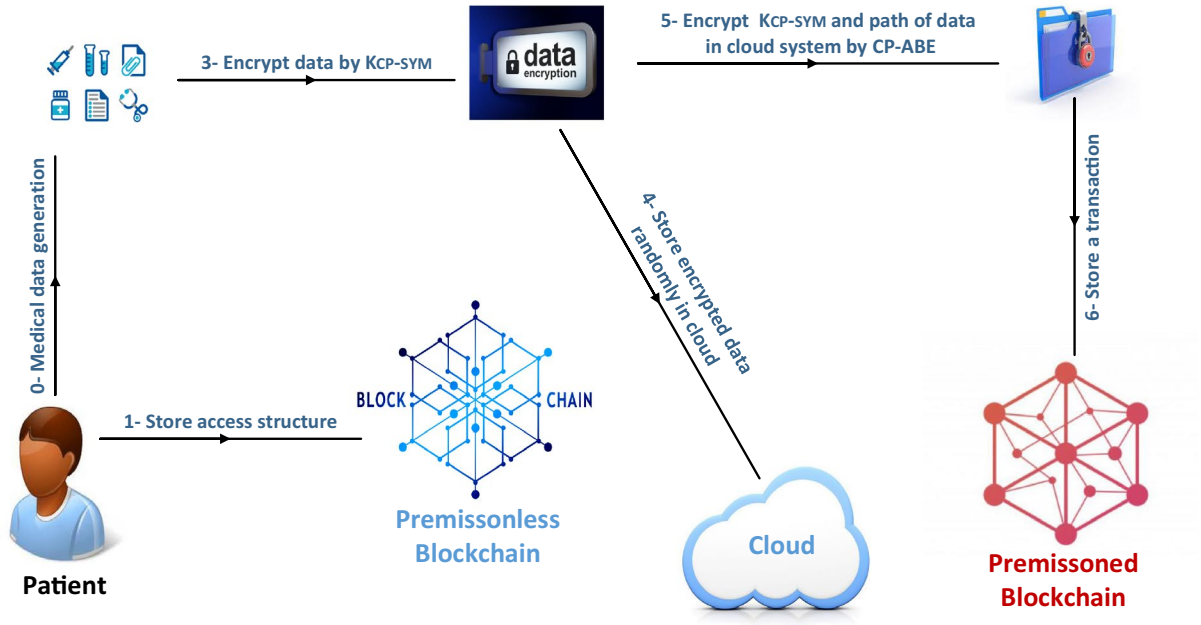

Fig. 5 How to register medical information by patients in MedSBA scheme

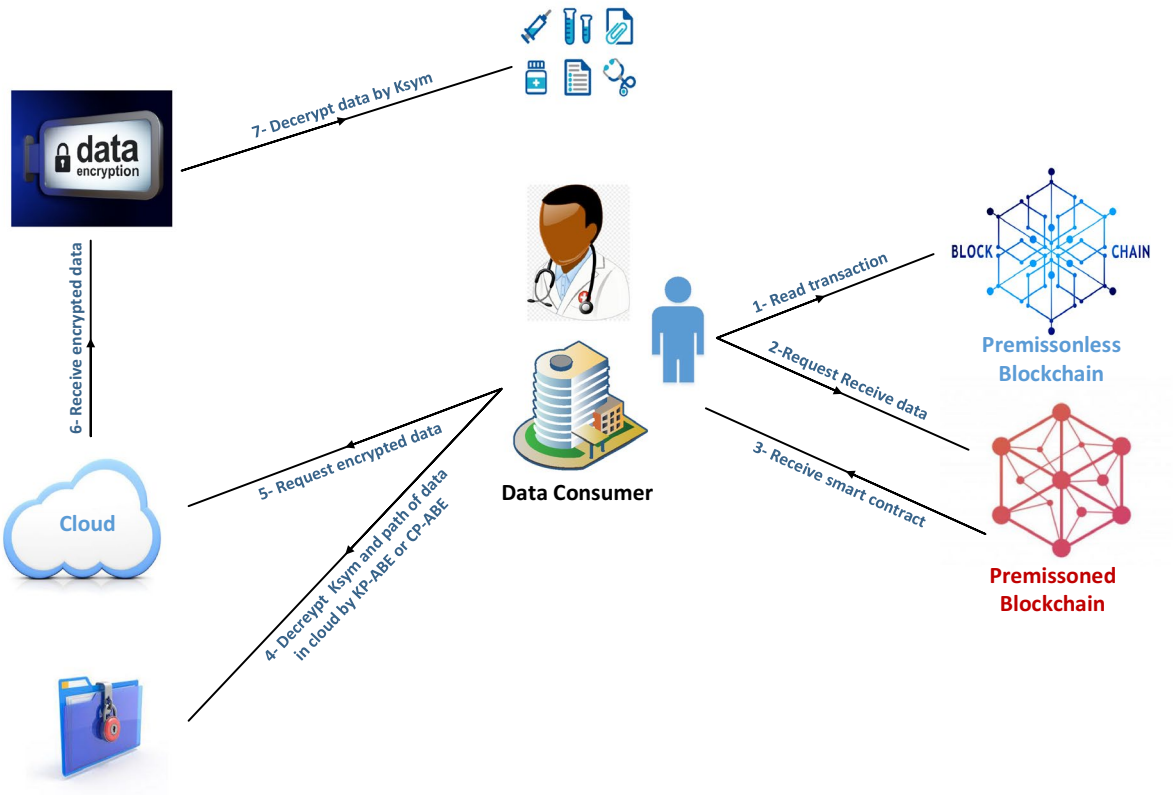

Fig. 6 How to request medical information in MedSBA scheme

implement the nodes setting the blockchains. Hence, there is one network infrastructure in our proposed scheme to set up blockchain with two different functionality. Patient PHR data is stored in an encrypted fashion and randomly in the cloud systems to increase system efficiency and due to the large amount of medical data.

Applying the public key encryption to encrypt data of large scale requires lots of time and computation cost; therefore, the PHR information is encrypted applying the AES symmetric cryptography algorithm by data producer entity and using the k_{sym} random key; then the k_{sym} key is encrypted by the attribute-based encryption and based on the access structure desired to data producer entity or the patient. The medical content producer entity encrypts the PHR data encryption key based on the determined access policy using the attribute-based cryptography so that data user entities can access the required medical information and ensure its accuracy as well. The entity sets the PHR data encryption key, the data storage path encrypted in the cloud, the PHR hash content, and the authorized access structure in an anonymous fashion in a transaction proportional to the blockchain structure. The entity then signs and transmits the transaction to a permissioned private blockchain. The medical content producer entity creates and anonymously distributes another transaction including a description and an authorized data access structure encrypted in a permissionless private blockchain to be accessible for all data user entities. The transaction validating nodes in a blockchain verifies all distributed transactions those of which able to achieve a specified vote number of blockchain nodes will be registered in the private blockchain by the leader node determined in the consensus process.

There are two types of medical information in this system, the EHR information regularly produced by a patient using related devices and sensors; the medical information depended on a determined patient, such as radiology images, prescriptions, insurance bills and so on produced by the hospital, laboratory or physician. The EHR information is encrypted and stored in the cloud by the patient himself; while the medical data generated by the hospital is encrypted by the hospital itself using encryption key encrypted based on patient access structure and stored in private blockchain along with data hash and storage path in the cloud. Therefore, two entities in the MedSBA system have authority to encrypt data, the hospital encrypting the medical data associated with the patient, and the patient encrypting the EHR registered data and part of his medical data he is interested in providing to other entities and his parents and friends.

The data encrypted by the hospital is encrypted using KP-ABE encryption. Hence, according to the permissible access structure for data decryption located in the private key generated by the KGC entity, specified entities will be authorized to access this data. Patients have no idea about such entities and even to be informed of which is not necessary for patients. However, patients register, in an authentic transaction in the blockchain, the attributes necessary for the entities interested in decrypting this data and the hospital is obliged to observe this access policy for decrypting such data. The hospital encrypts this data using the k_{kp-sym} random key and then encrypts that key based on the attributes specified by patients, using the KP-ABE algorithm.

The nodes of blockchain verify the access policy for data encryption predetermined by the patient and the access policy applied on the k_{kp-sym} key by the hospital and if they are the same data storage path and the hash of data will be registered in the private blockchain to be accessible for the considered entities. Simultaneously, a transaction including a brief description of and the structure of authorized access to data is distributed in the public blockchain. The process of medical data encryption generated by hospitals and data in high volume has been assigned to the hospital to facilitate and increase system efficiency (Fig. 4).

EHR data and some part of the information the patient wants to submit to particular entities, friends, and consultant physician is accurately determined based on patient desired access structure. The private keys in this section are generated and accessible for individuals and entities by the patient himself. Then each part of the information is encrypted by the k_{cp-sym} random key and k_{cp-sym} key encrypted based on the patient determined access structure together with data hash and authorized access structure is registered and stored in the blockchain to be used by other authorized entities (Fig. 5).

The entities tending to use medical data in addition to having a key proportionate to the structure of authorized access to the data to be able to decrypt k_{cp-sym} and k_{kp-sym} should be able to generate an authentic transaction in which is pointed to an unused transaction from the content producer. That is the content producer entity has not revoked the right to access its medical information, having that specific access structure yet. Smart contracts contribute to performing such a process. The inputs of this smart contract include an unused transaction in the permissionless blockchain, generated by the PK public entity, with a specific access structure, and a transaction with a registered access query, as well. The output of this smart contract is an authentic transaction in the permissioned blockchain, in which data storage path in the cloud and the k_{sym} symmetric key are encrypted, having been previously generated by the patient or hospitals and stored in the blockchain. Achieving the encrypted key information and data storage location makes data user entities provide an unused transaction to increase the functionality and facilitate the immediate access revocation process in the attribute-based encryption (Fig. 6).

4.1 Architectural method

There are six entities in the MedSBA system, KGC registration center, cloud storage system, blockchain network, data consumer entities, data-producing entities, and patients:

Production and registration center (KGC): This center determines and distributes the public parameters of the network. All medical data consumer entities such as hospitals, insurance institutions, medical research centers, etc. should register in this center. Then, the KGC center, given the properties of and the authorized access structure assigned to each entity (Γ_{kp}), generates private decryption keys appropriate to that access structure and provides them securely. Indeed, the KGC determines which encrypted messages each entity is authorized to access. The KGC also produces the signature keys and makes them available for data-producing centers securely.

Cloud storage system: Medical data is stored in an encrypted fashion in one or more cloud systems due to its large amount. The PHR information registering entities or patients can store data in an encrypted form in random places on the cloud systems, and then set the storage path and key available to the authorized data consumer entities. In case of possessing the encryption key, data consumer centers can decrypt the information they request from the cloud systems.

Blockchain: The MedSBA scheme applies two private blockchains, permissionless and permissioned, based on the PBFT consensus methods. Data storage path in the cloud system, data decryption key in an encrypted fashion, and data hash are stored in blockchain transactions. The nodes participating in a blockchain network are divided into two groups, validation nodes (vdN) to authenticate transactions submitted to a blockchain network and bookkeeping nodes (bkN) to register authentic transactions in a blockchain. VdN nodes as the systems of computers used in hospitals, insurance institutions, and health institutions verify the authenticity of the signature and the access structure provided on all transactions published on the network. Executing a PBFT consensus protocol, VdN nodes select a node as responsible for registration and storage of an authentic transaction in the blockchain. The bkN node stores the transaction in the blockchain, informing all network members of it. The member nodes of blockchain are also able to execute smart contracts to evaluate the authenticity of the access structure of entities, making data consumer entities access data encrypted key and storage path in the cloud.

The structure of blocks in this blockchain is to some extent similar to that in Bitcoin including a block number, the previous block hash, root of the Merkel-tree, and time stamp. Due to replacing the PoW consensus method by PBFT difficulty target and nonce are removed from the structure of such blocks. It is the previous block hash and time stamp that cause the integrity of blocks and prevent them from any changes absolutely visible if any; and the root of Merkle-tree including all transactions hash existing in block guarantees block integrity.

Data producer entities: Such as patients, hospitals, laboratories, and other health entities that produce PHR data associated with patients.

Data consumer entities: There are two groups of data consumer entities as follows: the legal entities for consuming medical data such as hospitals, insurance institutions, and medical research centers analyze or use patient medical data to advance their interests. Research entities should use patient medical data in a way not to violate patient privacy; however, medical data authenticity and connection with patients are of great importance to the insurance institutions and treatment centers. The second group includes all entities such as friends, parents, and consultant physicians to whom a patient voluntarily tends to make some part of his medical information available. Certain entities with research goals may also request to use patient medical information; all these individuals and entities can access patient information based on the access structure (Γ_{cp}) that the patient himself determines for them.

Patients: Are the individuals whose medical information is collected and provided to the PHR data consumer entities. Privacy-preserving in distributing medical data is of great importance for patients; however, referring to health centers, they want to be easily informed of their medical history to submit it to the health centers.

4.2 Security requirements

The GDRP is a regulation that protects the privacy of all individuals. Thus, business processes that manage personal information must store personal information using pseudonymization or anonymization and maximize confidentiality by default, so that data is publicly available without explicit consent, and can not be used without individual additional information to identify individuals. No personal information can be processed unless lawfully authorized by the specified regulations, or controller or data processor, explicitly and voluntarily from the owner of the data. The owner of the data can cancel this permission at any time.

Hospital servers and patient computers are considered as semi-trusted entities in the network. They honestly implement the protocol, but with no permission are curious to access the user's health information. The external attackers can also listen to the information transmitted to the public channels, such as PHI encrypted information and medical data description. Medical information registration should meet the following security attributes according to the literature existing in the Medical Record

Registration system (Aitzhan and Svetinovic 2016). Hence, we intend to achieve the following goals:

Data security and access control: Since privacy preserving in PHI is of great importance, achieving data security requires well-preserving information confidentiality and integrity, data auditability, and access control. Cryptography and digital signature regularly guarantee data confidentiality and integrity. Data auditability and access control should be met to ensure all PHI data access activities are precisely controlled and observed by the data producer entity and the owner. In MedSBA, data confidentiality can be met by data cryptography using AES and access control can be met using ABE cryptography and the permissioned private blockchains where medical information encryption key and data storage path in the cloud are located and the permissionless private blockchain where PHI data description and authorized access structure are placed.

Patient anonymity: The medical information storage system should guarantee the anonymity of identities and linkability of the users to preserve privacy. Here unlinkability means that the attacker is not able to recognize whether two or more PHI flows are issued from one source or more different sources. According to a blockchain-based system, an attacker cannot recognize the real identity of patients through a simple analysis of transactions.

No online center required: A medical information storage system should not require a centralized online process to minimize communication costs. Considering the blockchain distributed technology used in the MedSBA scheme, there is no centralized and online entity for network control.

Perfect forward secrecy: In perfect forward secrecy, the previous information of sessions should not be visible by revealing user private key information. The MedSBA scheme enables users to sign the new transactions by a new cryptography key, so the previous information of sessions will be invisible.

4.3 Introduction to the details of proposed scheme

The attributes in the attribute-based encryption have the same importance level and no superiority to each other. While in practice, some of the attributes are of more importance than the rest. For instance, the expertise of a doctor is more important to which hospital the physician affiliated or what his features may be. Hence, the proposed MedSBA scheme applies ABE scheme based on key policy and hierarchical threshold attribute-based encryption to encrypt data by the legal entities such as hospitals (Wang et al. 2016; Huang et al. 2017; Tassa and Dyn 2009; Deng et al. 2014; Sahai and Waters 2005) and ABE scheme based on ciphertext policy CP-ABE proposed by Bethencourt et al. (2007) to encrypt patient data.

Our proposed scheme includes six phases, determining attributes and access structure, initial system setup, encrypting PHR data, decrypting and using PHR data, consensus and verifying transactions in the blockchain, and revoking the right to access. Table 1 presents the used symbols.

4.3.1 Determining attributes and access structure

Choosing a set of attributes and appropriate access structure is the first step in establishing an ABE system. The attributes set (U) in our proposed system is divided into two separate sets KP-ABE and CP-ABE. The medical properties such as doctor and patient profiles are used to define a time-based attribute set (γ_{kp}) to do KP-ABE. A medical profile can include general practitioners, surgeons, nurses, pharmacies; and patient profiles age, gender, and individual identification number. We create an access structure (Γ_{cp}) proportional to the attributes such as friends, family, medical advisers, and health care centers for CP-ABE.

Suppose Γ represents the tree that represents an access structure. Each inner node (non-leaf node) of a tree is a threshold gate described by a threshold value and its children. Given num_x be the number of children and k_x, the threshold value of node x, then $0 < k_x < num_x$. In this case, when $k_x = 1$, the threshold is OR, and when $k_x = num_x$,

Table 1 Symbols used in MedSBA scheme

Notations	Description
KGC	Key generation Center
γ_{kp}, γ_{cp}	Medical features for KP-ABE and CP-ABE respectively
Γ_{kp}, Γ_{cp}	Medical access tree for KP-ABE and CP-ABE respectively
MK_{kp}, MK_{cp}	Master secret key for KP-ABE and CP-ABE respectively
K^i_{pr}, K^i_{pub}	The ith private and public key of user respectively for signing and verifying blockchain transctions
ITx, PTx, UdTx	Information transaction, permission transaction and used data transaction respectively
K_{kp-sym}, K_{cp-sym}	Random AES key for user data encryption in KP-ABE and CP-ABE respectively
vdN, bkN	Validation and bookkeeping node in blockchain respectively

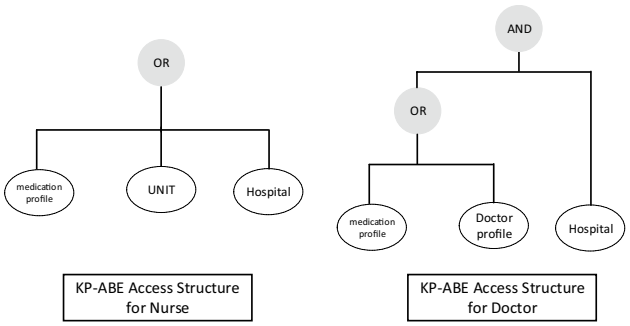

Fig. 7 Access structure for KP-ABE encryption

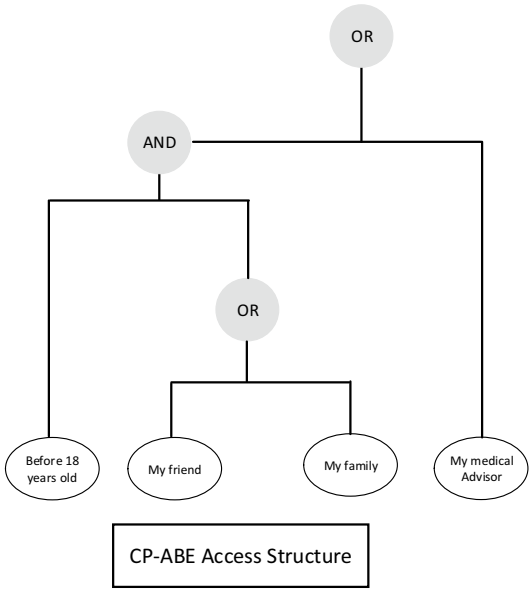

Fig. 8 Access structure for CP-ABE encryption

the threshold value is AND. Each leaf node x of the tree is described by a property and a threshold value $k_x = 1$.

Accordingly, we divide the attributes into two separate domains, the public domain refers to the PHR information inherent characteristics, and the private domain refers to personal information to identify the individuals existing in the PHR system. For KP-ABE, each access structure Γ_{kp} specifies what information can be accessible for an entity with specific attributes. For instance, a nurse can access the information labeled with characteristics of the determined nurse, hospital, and ward. Figure 7 presents some examples of access structures for different roles. Therefore, each set, according to its requirements, can generate its desired structure to access the determined information.

The access structure Γ_{cp} in the CP-ABE specifies the entity, which can decrypt an encrypted text with specific labels. A patient can create an access structure as shown in Fig. 8, for example, to make his blood pressure information accessible for the hospital physicians and his parents, as well, if he is a minor. Consequently, a patient can produce any access structure for each section of his medical information.

We use ABE as a building block of our proposed scheme. That is because ABE not only offers fine-grained access control similar to RBAC or ABAC but also enforces data protection against the semi-trusted server. Therefore all hospitals and their authorized personnel who can register medical information in the blockchain must visit the KGC once and be authenticated by the KGC based on their authorized features such as those shown in Fig. 7, then the KGC delivered them the keys corresponding to their authorized features securely. The patient also provides the private keys appropriate to the structure of their access to the institutions that the patient wishes to access their medical information such as those shown in Fig. 8, and then delivered these keys securely. Further details of this process are given below.

4.3.2 System initial setup phase

The initial setup phase has two separate sections, one carried out by the KGC to provide the communication between hospitals and the authorized medical entities, and the other is performed by patients to contact with medical institutions, counseling physicians or individuals.

KGC initial setup phase: This phase consists of two sections, defining general parameters for the system and producing MK_{kp} main keys to KP-ABE [flow (0–1) in Fig. 11].

Defining general parameters for the system: KGC determines the general parameters for the system, including hash function, elliptic curve parameters, and bilinear mapping, and introduces them to the entire network.

- Suppose G_1 is a cyclic additive group generated by P and G_2 is a multiplicative cyclic group. G_1 and G_2 have the prime-number order q. Suppose $e : G_1 \times G_1 \longrightarrow G_2$ is a bilinear pairing.
- Suppose $H_1 : \{0, 1\}^* \rightarrow G_1$ is a map to point and $H_2 : \{0, 1\}^* \rightarrow Z_q^*$ is a secure hash function and $H_3 : G_1 \rightarrow \{0, 1\}^*$.

Producing MK_{kp} main keys to KP-ABE: This algorithm is implemented by the KGC key generation center to produce encryption keys appropriate to legal entities such as hospitals.

- The KGC defines a set of U attributes and divides all the attributes into the subsets $U_0, U_1, ..., U_m$ according to their importance level.
- The KGC selects the random numbers $t_0, t_1, ..., t_{|u|}, y \in Z_p$ as the secret key MK_{kp}.

- The KGC selects the generator g in G_1 group and calculates the following values: $T_1 = g^{t_1} modq, ..., T_{|u|} = g^{t_{|u|}} modq, Y = e(g,g)^y modq$.
- The system public parameters are $Params = \{G_1, G_2, e, g, T_0, T_1, ..., T_{|u|}, Y\}$ distributed by key KGC generation center.
- The KGC selects a random polynomial q of $m-1$ degree such that $q(0) = y$.
- The KGC calculates the value of $D_i = g^{\frac{q(i)}{t_i}} modq$ for any attribute i existing in γ_{kp}.
- The KGC confidentially delivers the private key components, $\{D_i\}_{i \in y_{kp}}$ to the user with the attributes γ_{kp}.

System setup phase for patients: This phase also has two steps, production of MK_{Cp} main keys for CP-ABE, and public and private keys for signing transactions by the patient [flow (0–2) in Fig. 11)].

Producing MK_{Cp} main keys to CP-ABE: This algorithm is performed by the patient to generate data decryption keys for the individuals or entities for which the patient inclined to provide his medical information.

- The patient defines a set of his desired attributes in the form of $U = \{1, 2, \ldots, n\}$.
- The patient selects two random numbers α and β from $\mathbb{Z}_p$.
- The patient public parameters PK are as follows: $PK = \{G_0, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha}\}$ distributed by the patient.
- The patient MK_{Cp} secret key is (β, g^{α}).

The patient produces a private key corresponding to γ_{cp} attribute set by MK_{Cp} secret key as follows:

- The patient produces a random number $r \in \mathbb{Z}_p$ and then the random numbers $r_j \in \mathbb{Z}_p$ for every attribute j member of γ_{cp} set.
- The patient calculates the key proportional to the attribute set γ_{cp} as follows: $Sk = (D = g^{(\alpha+r)/\beta} modq, \forall j \in \gamma_{cp}, D_j = g^r . H_1(j)^{r_j} modq, D'_j = g^{r_j} modq)$
- The patient provides this key set securely to the individuals and entities of his choice.

Producing public and private keys for signing transactions: The user produces his own public and private keys for signing his desired transactions. The user anonymity will be threated, if the user signs all transactions transmitted to the network using one private key, so the user should sign each transaction or a group of transactions using a new private key based on the anonymity level of his choice. It would be difficult and costly for the user to generate and maintain a large number of private and public keys. Therefore, the MedSBA scheme uses the attribute of hierarchical key generation to produce signature keys, that is the user only generates a seed based on which his required private and public keys are generated; hence, it is required to securely store just one seed making the confidentiality of user private key maintenance increase.

- The user selects two random values of $k, x \in_R Z_p^*$ and then securely stores x as the seed of his private key.
- Whenever it is required to sign a transaction, the user will calculate his ith private key as follows: $K_{pr}^i = x + H_2(k||i) modp$ then computes the public key corresponding to it as follows: $k_{pub}^i = k_{pr}^i G_1 = xG_1 + H_2(k||i) G_1 modp$.
- $H_3(K_{pub}^i)$ is considered as the user pseudo identity in the transaction.

The Pseudo-random property of hash functions having multi different public keys makes it impossible to communicate with each other and recognize whether the seed of their producer is the same or different, so the unlinkability property in the communications of the users is well preserved and the anonymity of the users is guaranteed (Fig. 9).

4.3.3 PHR data encryption phase

There are two types of data for encryption in our proposed scheme; medical data produced by the hospital affiliated to a patient but encrypted by the hospital and EHR data or that which the patient wants to provide to other individuals and entities. Medical data producer entity after encrypting data registers a transaction including a brief description and access conditions of the produced data in the permissionless blockchain, then registers another transaction containing data storage path and k_{sym} encrypted key in the permissioned blockchain as well. Data consumer entities should also register a transaction in the permissioned blockchain to access data encryption key and storage path to set up a smart contract.

Different types of MedSBA transactions: Transactions in the Bitcoin include a sender address (sender public key), a recipient address (receiver public key), and the transmitted Bitcoin value, with a signature by a sender private key.

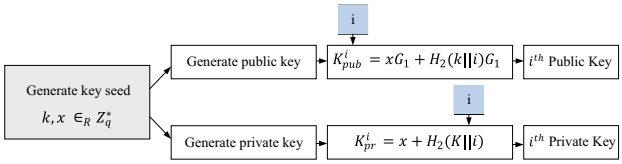

Fig. 9 Signature hierarchical key generation

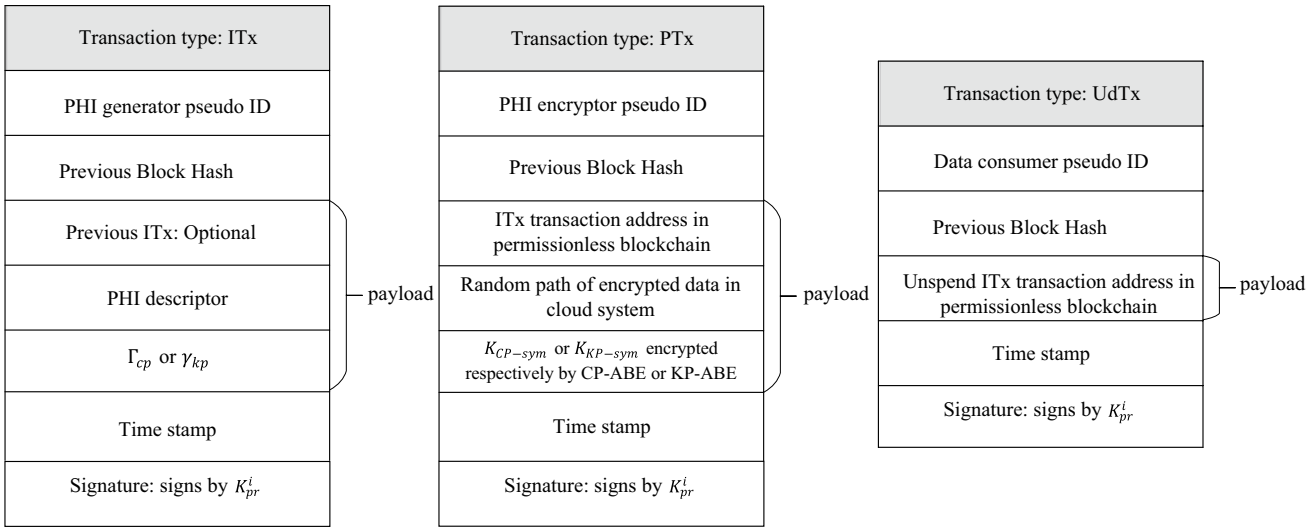

Fig. 10 Structure of transactions in MedSBA scheme

However, there are three transaction types with different fields in MedSBA system, the structure of which is shown in Fig. 10.

Information transaction (ITx): This transaction is registered by patients in the permissionless blockchain to inform of medical data content including the registered medical data summary, data access structure, the pseudo-identity of medical content producer, and his signature on all transaction information.

Permission transaction (PTx): This transaction is registered by hospitals or patients in the permissioned blockchain to send the encrypted medical data and the right to the authorized access of users. This transaction includes the random path of data storage encrypted in the cloud, data symmetric cryptography key encrypted by ABE, and the signature of the transaction generator on this content.

Used data transaction (UdTx): This transaction is registered by medical data consumer entities in the permissioned blockchain to access medical information encrypted in the cloud. This transaction includes the pseudo-identity of medical data consumer entities, the signature of medical information client, and transactional address in the permissionless blockchain to which the user requests access.

Data encryption by hospitals: A hospital encrypts the medical data related to its patients based on the attributes announced by patients and according to KP-ABE method so that other legal entities can access, which includes the following phases:

- The patient identifies the attributes necessary to decrypt his PHR data provided to the hospital from the U set (γ_{kp}).
- The patient generates an appropriate pair of public and private keys based on the method stated in Sect. 4.3.2 to sign the transactions (K^i_{pr}, K^i_{pk}).
- The patient generates ITx transaction of the attributes necessary for the encryption (γ_{kp}) and a brief description of the information and signs it by the private key K^i_{pr}.
- Then the patient stores the transaction ITx in the permissionless blockchain [flow (1–1) in Fig. 11).
- The hospital generates a random key K_{kp-sym} for data encryption and using AES algorithm encrypts the data related to patient p_i.
- The hospital encrypts the key K_{kp-sym} using KP-ABE method based on the attribute (γ_{kp}) registered by the patient in the transaction in the permissionless blockchain.

Signing transactions: ECDSA digital signature on the standard elliptic curve "secp256k1" is used in MedSBA scheme to sign the transactions registered in a blockchain. K^i_{pr} private key length in this signature is 256 bit and K^i_{pub} public key length is equal to 512 bit which using compression technique in storing the elliptic curve points will be 257 bit. The signature output length equals to 512 bit as well. The elliptic curve security level secp256k1is expected to be 2^{128}.

Encrypting K_{kp-sym} using KP-ABE method: The hospital encrypts K_{kp-sym} key under the set of (γ_{kp}) attributes specified by the patient as follows:

- The hospital chooses a random integer $s \in_R Z_p$.
- The hospital computes $E_i = T_i^s modq$ and $E' = K_{kp-sym} Y^s$ values for all attributes existing in γ_{kp}.

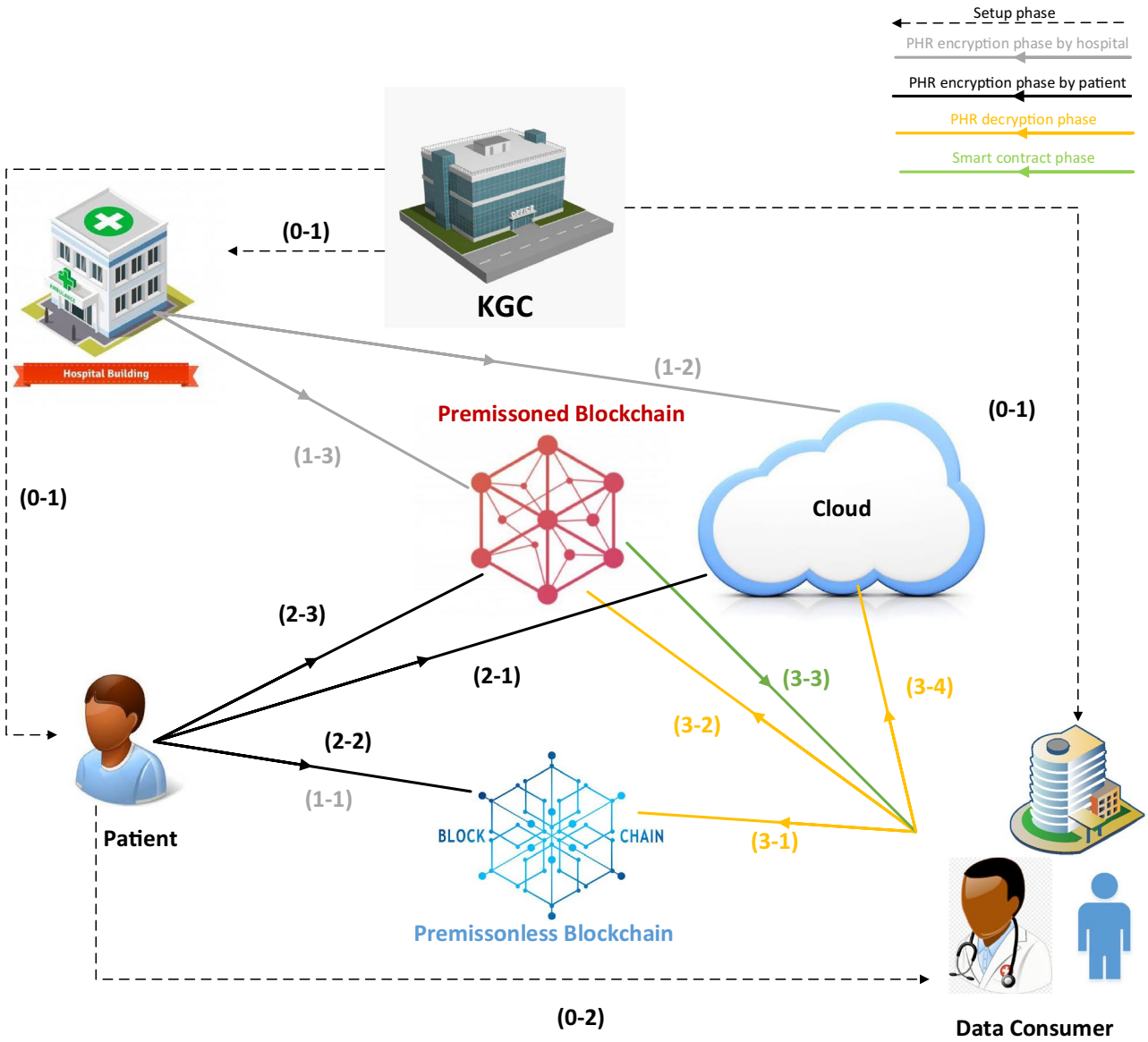

Fig. 11 The MedSBA proposed scheme architecture

- The hospital encrypts k_{kp-sym} key in $E_{kp} = (\gamma_{kp}, E' = k_{kp-sym} Y^s, \{E_i = T_i^s\}_{i \in \gamma_{kp}})$ form.
- The hospital stores patient medical data encrypted by k_{kp-sym} key in random locations in the cloud storage system (Flow (1–2) in Fig. 11).
- The hospital generates a PTx transaction including E_{kp} and data storage path in the cloud and storing it in the private blockchain [flow (1–3) in Fig. 11].
- The vdN nodes existing in the private blockchain evaluate the PTx transaction and in case the attribute used in k_{kp-sym} encryption is the same as the attribute announced in its corresponding ITx transaction registered by the patient in the public blockchain, then this transaction will be registered as an authentic transaction in the blocks of the private blockchain.

Data encryption by the patient: The patient applies CP-ABE cryptography to provide all or part of his medical information to other individuals and entities based on his preferred access policy as follows:

- The patient generates K_{cp-sym} random key to encrypt EHR data or the information he wants to provide to other entities.
- The patient encrypts his desired data using K_{cp-sym} key and AES algorithm.

- The patient stores the encrypted data in random places in the cloud [flow (2–1) in Fig. 11].
- The patient determines (Γcp) access structure based on which entities or individuals can use the information with which attributes.
- The patient encrypts K_{cp-sym} key based on the preferred access structure (Γcp) using CP-ABE encryption.

Encrypting K_{cp-sym} key using CP-ABE method: The patient encrypts K_{cp-sym} key based on (Γ_{Cp}) access structure as follows:

- First, patient for each node x (including leaves) in the access structure (Γcp), chooses a random polynomial q_x of $d_x = k_x - 1$ degree, selecting these polynomials in the top-down method, starting with the root node R, as follows:
  - For the root-node polynomial R, the patient first chooses a random number $s \in Z_p$ sets $q_R(0) = y$, and the rest of points of this polynomial d_R are selected randomly.
  - For other nodes x, patient sets $q_x(0) = q_{parent(x)}(index(x))$ and the rest of points of this polynomial d_x are selected randomly.
  - Patient selects the other d_x point of the polynomial randomly.
- If Y is the set of leaf nodes in the access structure (Γcp), then the cipher-text of $K_{cp-sym} \in G_1$ will be calculated under the access structure (Γcp) as follows:

$$E_{cp} = (\Gamma_{cp}, \tilde{C} = K_{cp-sym} e(g,g)^{\alpha s}, C = h^s, \\ \forall y \in Y : C_y = g^{q_y(0)}, C'_Y = H_1(att(y)^{q_y(0)})) \quad (4)$$

- The patient produces an appropriate pair of public and private keys based on the method described in Sect. 4.3.2 (K^i_{pr}, K^i_{pk}) to sign transactions.
- The patient then generates an ITx transaction including the authorized access structure (Γcp) and a brief description of the stored data and signs it with the private key K^i_{pr} and records the transaction in the permissionless blockchain [flow (2–2) in Fig. 11].
- The patient also generates a PTx transaction including the data storage path in the cloud and the encrypted key K_{cp-sym} using CP-ABE encryption and signs it with the same private key K^i_{pr} and registers in the permissioned blockchain [flow (2–3) in Fig. 11].
- The nodes existing in the permissioned blockchain evaluate the PTx transaction and in case the attribute used in K_{cp-sym} encryption is the same as the attribute announced in its corresponding ITx transaction registered by the patient in the permissionless blockchain, then this transaction will be registered as an authentic transaction in the blocks of the permissioned blockchain.

4.3.4 Decryption phase and using PHR data

Observing the transactions registered in the permissionless blockchain, the entities willing to use medical data will perform the following process, in case of possessing the attributes required to receive the information based on the authorized access structure registered in the corresponding ITx transaction [flow (3–1) in Fig. 11]. The consumer entity registers an UdTx transaction in the permissioned blockchain requesting the use of specific medical data [flow (3–2) in Fig. 11].

- Then it executes a smart contract with two inputs, the UdTx transaction registered by the entity for using medical data and a transaction including a general description and the access structure of the data in the permissionless blockchain (ITx transaction) [flow (3–3) in Fig. 11].
- The nodes of the permissioned blockchain execute a smart contract.
- By executing a smart contract, the vdN nodes existing in the permissioned blockchain consensus process evaluates that if the ITx transaction addressed in the permissionless blockchain is not consumed (meaning the patient does not register a transaction of spend type with its resource in the permissionless or permissioned blockchain) then the output of the smart contract will be authentic and the PTx transaction corresponding to the ITx transaction registered in the permissionless blockchain delivered to the client entity. The PTx transaction includes data storage path and its encrypted key having the attributes proportional to the data client entity.
- Then uploading the encryption data from the cloud-based on the specific path in the PTx transaction caused by the smart contract, the data consumer entity decrypts KP-ABE or CP-ABE to access the data content [flow (3–4) in Fig. 11].

Decrypting K_{kp-sym} using KP-ABE method: Data recipient with γ'_{kp} attributes decrypts E_{kp} cipher-text under γ_{kp} attributes if $|\gamma_{kp} \cap \gamma'_{kp}| \geq m$ with its key as follows:

- Selecting m number of γ'_{Kp} attributes having share with γ_{kp} and placing it in the set of S.
- Then using m attributes and polynomial lagrange coefficients $\triangle_{i,s}$ the following computation is made:

$$E' / \prod_{i \in \gamma'_{kp}} (e(D_i, E_i))^{\triangle_{i,s}(0)} \quad (5)$$

Approving decryption accuracy: Equation (5) is correct because based on the definition of the attributes γ'_{kp}, if a user with the set of γ_{kp} attributes meets all threshold conditions, having the same property, the user can do the decryption as follows:

$$\begin{aligned} E' / \prod_{i\in\gamma'_{kp}} (e(D_i, E_i))^{\triangle_{i,s}(0)} \\ &= k_{kp-sym} e(g,g)^{sy} / \prod_{i\in\gamma'_{kp}} (e(g^{\frac{q(i)}{t_i}}), g^{st_i})^{\triangle_{i,s}(0)} \\ &= k_{kp-sym} e(g,g)^{sy} / \prod_{i\in\gamma'_{kp}} (e(g,g)^{sq(i)})^{\triangle_{i,s}(0)} \\ &= k_{kp-sym} \end{aligned} \tag{6}$$

Decrypting K_{cp-sym} using CP-ABE method: Receiving the E_{cp} cipher-text inputs including a Γ_{Cp} access structure and an MK_{Cp} private key (a key for the set of γ_{cp} attributes) and the public parameters of PK system, data recipient decrypt as follows:

Suppose x is a leaf node and $i \in \gamma_{cp}$ then the function value is calculated as follows: The decryption function of the cipher-text $E_{cp} = (\Gamma_{cp}, \tilde{C}, C, \forall y \in Y : C_y, C'_y)$ admits as inputs the MK_{Cp} private key dependent on the set of γ_{cp} attributes and the node x of Γ_{cp} structure. The function is defined for different x that $i = att(x)$, as follows:

$$\begin{aligned} DecryptNode(E_{cp}, MK_{Cp}, x) &= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} \\ &= \frac{e(g^r.H_1(i)^{r_i}, g^{q_x(0)})}{e(g^{r_i}.H_1(i)^{q_x(0)})} = e(g,g)^{rq_x(0)} \end{aligned} \tag{7}$$

And if $i \notin \gamma_{cp}$ then $DecryptNode(E_{cp}, MK_{Cp}, x) = \perp$.

And if x is an internal node, first it calculates the function $DecryptNode(E_{cp}, MK_{Cp}, z)$ for all z nodes the children of x and stores it as F_z , then willingly places K_x number of z child nodes, where $F_z \neq \perp$ in the S_x set. If there were not such a set the function brings back the $\perp$ value, otherwise the following computations will be done where $i = index(z)$ and $S'_x = \{index(z) : z \in S_x\}$.

$$\begin{aligned} F_x &= \prod_{z\in S_x} F_z^{\triangle_{i,s'_x}(0)} = \prod_{z\in S_x} (e(g,g)^{r,q_z(0)})^{\triangle_{i,s'_x}(0)} \\ &= \prod_{z\in S_x} (e(g,g)^{r,q_{parent(z)(index(z))}})^{\triangle_{i,s'_x}(0)} \\ &= \prod_{z\in S_x} (e(g,g)^{r,q_x(i).\triangle_{i,s'_x}(0)}) = e(g,g)^{r,q_x(0)}. \end{aligned} \tag{8}$$

Having been defined, the function DecrypNode is supposed to call the decryption algorithm of the function $DecryptNode(E_{cp}, MK_{cp}, R)$. If the Γ_{cp} access structure is met by the attributes of γ_{cp} set the function value is equal to:

$$DecryptNode(E_{cp}, MK_{Cp}, R) = e(g,g)^{rqR}(0) = e(g,g)^{rs}. \tag{9}$$

Doing the following computations it will simply be possible to access the plain-text.

$$\tilde{C}/(e(C,D)/A) = \tilde{C}/(e(h^s, g^{\alpha+r/\beta}/e(g,g)^{rs})) = K_{cp-sym} \tag{10}$$

4.3.5 Consensus and evaluation phase of transactions in blockchain

The consensus mechanism is considered to be the core of blockchain technology because of determining whether a new block is authentic and maintains the network records or not. Hence, the consensus process affects the security and reliability of the whole system. Both the blockchains used in the the MedSBA system are of the private blockchain type and how to access one is through permissioned form and the other permissionless.

The node members of each blockchain maybe different computers of the hospital, patients, or other medical entities select a node, at each interval, to register a final block in the network through the implementation of the BPFT-based consensus protocol. The selected node is responsible for registering the transactions verified by most network nodes in the final block of the blockchain. Evaluating the registered transactions in the network, all nodes of the blockchain network verify the signature of these transactions. The details of the PBFT-based consensus process used in the MedSBA system are similar to that described in Sect. 6.3. Therefore, the repeated blocks in the network will be authentic, if more than two-thirds of all participants in the consensus process approve them.

A transaction in the permissionless private blockchain is accurate that has an authentic signature and right reference to the previous hash block. Hence, the member nodes of a blockchain verify the authenticity of a transaction merely through evaluating the accuracy of its signature and the validity of network previous hash block.

An accurate transaction in the permissioned private blockchain in addition to the accuracy of the signature of its generator and the authenticity of the network previous hash block should include an unused transaction in the permissionless private blockchain and the transaction content should be encrypted compatible with the access structure addressed in the transaction; therefore, the vdN member nodes of the permissioned blockchain in addition to verifying the accuracy of the signature of the transactions registered in this blockchain should evaluate the authenticity of the transaction referred from the permissionless blockchain as well as the compatibility of its access structure in the cryptography of the transaction content registered in the permissioned blockchain.

4.3.6 Updating and revoking the right to access

It is not easily and rapidly possible to alter the access structure and remove the attributes allocated to a user in the attribute-based encryption while facing numerous challenges. However, in the MedSBA system, enabling a user to revoke or for any reason alter the access structure created for encrypting certain data requires consuming the transaction in which the access structure already registered for specific data in the public blockchain.

How to consume a transaction is such that the data producer source (maybe a patient or hospital) creates a new transaction with the private key used to sign the same previous transaction in which the authorized access structure was set. Moreover, the user should refer to the previous transaction in the new one. The verifying nodes of the blockchain can easily be informed of the use of a transaction within another transaction by evaluating the structure of Merkle-tree. Therefore, if so, having been canceled by the producer, the transaction is no longer valid. Hence, the output of the smart contract fails, as a result, the transaction wherein located data storage path and its encrypted key, will not be delivered to the user. In which case, in spite of having an authorized access structure in the ABE encryption, the user cannot access data due to the policy change of the data producer entity.

Accordingly, using the blockchain technology and the concept of the consumed transaction, we improve the process of revoking and updating the right to access in the ABE encryption used in the MedSBA scheme.

5 Security analysis of the proposed scheme

How the MedSBA scheme can efficiently match the objectives designed in the "architecture model" is analyzed in this section. To this end, we formally demonstrate the security of the CP-ABE and KP-ABE encryption schemes used in this architecture and show that these schemes in the Random Oracle model have provable security. We also prove the precise operation of the protocol in BAN logic and demonstrate the fact that the protocol correctly achieves its security goals.

PHI data integrity: The main attribute of a blockchain ensures the security of the data in our proposed scheme, in other words, the data stored in the blockchain is immutable unless there would be a threat of 51% attack. The blockchain structure shows that data is unchangeable and untraceable. Meaning blockchain can support secure data management on the network. Therefore, it is not possible to change the PHR data on the network.

The PHI data privacy: Regarding the PHI data is encrypted by the K_{sym} key and in random places from the cloud, the K_{sym} key and the data storage path should be available to access this information. Considering the K_{sym} key is encrypted using the CP-ABE or KP-ABE method based on the access structure determined by the producer of the medical content, only the entities having an appropriate attribute and authorized access structure can decrypt the PHI data. Since the encrypted key and data storage path are stored in the permissioned blockchain, so only the entities executing a smart contract in the permissioned blockchain can access the data storage path in the cloud.

Instantly revoking the right to access the PHI information: Regarding the entities consuming medical content should provide an unused transaction with a structure of authorized access to data so a medical content producer at any time can register a transaction in a blockchain to change or revoke the right to access the PHI data resulting in fine-grain access control on the PHI information.

User anonymity: The proposed scheme preserves user anonymity regardless of data security. Since the transactions signed by pseudo identities each of which can be unique to each transaction register the PHI data in a network, it is not possible to establish any connection between the actual identity of a patient and the PHI information and no association between different PHI data as well. According to the method mentioned in Sect. 4.3.3, each patient generates a pair of public and private keys separate from his previous keys to sign each transaction and then sign the transactions with a pseudo-identity and the new key.

5.1 Security proof of the KP-ABE encryption scheme

We demonstrate the security of the cryptography used in the MedSBA scheme in the selected identity, given the difficulty of the DMBDH problem; and show that the encryption scheme presented in the proposed security game is secure, assuming the impossibility of solving the DMBDH problem (Bayat et al. 2019b).

Assume that A is the attacker who with the probability ϵ is victorious in the game proposed for the KP-ABE encryption scheme. Then, using the attacker A, the challenger C is designed to solve the DMBDH problem with the probability $\epsilon/2$.

Suppose that the challenger C has received a random sample $(g, A = g^a, B = g^b, C = g^c, Z) \in G_1 \times G_2$ from the difficult problem of DMBDH. In the following, we will show how the Challenger C can get the solution to the DMBDH problem, using the attacker A during the game. Modeling of the provided game is as follows:

Setup: The challenger C sets the Y parameter to $Y = e(g, g)^a$, and determines the values of T_i for each i attribute in the system as follows:

- If $i \in \alpha$, then chooses a random number $\beta_i \in Z_p$ and sets T_i equal to $C^{\beta_i} = g^{c\beta_i}$.

- Otherwise, it chooses a random number $\omega_i \in Z_p$ and sets T_i equal to g^{ω_i}.
- Then delivers the general parameters to A.

Phase 1: At this step, A can request a private key for several attributes γ'_{kp} provided that their sharing with γ_{kp} does not apply to at least one of the threshold conditions. In other words, there must be $0 \le i \le m$ for which we have $|\cup_{j=0}^{i} \gamma_i \cap \cup_{j=0}^{i} \gamma'_i| \ge k_i$. Given the set attribute γ'_{kp} satisfies such a condition. The challenger C generates the private key for γ'_{kp} attributes as follows:

- Defining α equal to $\gamma'_{Kp} \cap \gamma_{Kp}$.
- Defining an inefficient attribute $0 \in u_0$.
- Determining the value α' to $|\alpha'| = k_m - 1, \alpha \subseteq \alpha', \alpha' \subset \gamma'_{kp}$ and the attributes existing in $\alpha' \bigcup \{0\}$ satisfy all threshold values.
- Defining the set S equal to $\alpha' \bigcup \{0\}$ value.
- Computing the components of the private key for the attributes $i \in \alpha'$ as follows:
  - If $i \in \alpha$, then selects a random number $s_i \in Z_p$ and then calculates the value $D_i = g^{s_i}$.
  - If $i \in \alpha' - \alpha$ then selects a random number $\lambda_i \in Z_p$ and then computes the value $D_i = g^{\frac{\lambda_i}{\omega_i}}$.

Indeed, the challenger C implicitly defines a $q(x)$ polynomial of degree $m-1$ by choosing $m-1$ random point together with the point $q(0) = a$ so that if $i \in \alpha$ the value of the function will be $q(i) = c\beta_i s_i$ and for the $i \in \alpha' - \alpha$ attributes the value of the function is equal to $q(i) = \lambda_i$. C generates the components of the private key compatible with the attributes $i \in ID' - \alpha'$ as follows: $D_i = g^{\frac{q(i)}{\omega_i}}$

Therefore, according to the above method, the challenger C could generate a private key for the attribute γ'_{kp} based on the original scheme.

Query: The attacker A sends two messages M_0 and M_1 having identical lengths to the challenger C. Then C randomly selects a bit v and using the attribute γ_{kp} encrypts the message M_v and sends the cipher-text E_{kp} to A. The ciphertext is as follows:

$$E_{kp} = (\gamma_{kp}, E' = M_v Z, \{E_i = B^{\beta_i}\}_{i \in ID}) \tag{11}$$

Phase 2: At this step, similar to Phase 1, A can have the same requests and C can respond in the same way.

Guess: At this point, A returns the value of the bit v' as the answer. If $v = v'$, then the challenger will return the value one, representing Z is equal to the value $e(g,g)^{ab/c}$. Otherwise, it returns the value zero to represent Z as a random integer in the group G_2. At present, we show that if A in the above game wins with the probability ε then C can solve the problem DMBDH with the probability $\varepsilon/2$.

If $z = e(g,g)^{ab/2}$, then $E' = M_v e(g,g)^{ar'} = M_v Y^{r'}$ and for each attribute $i \in \gamma_{Kp}$, will be $E_i = B^{\beta_i} = G^{b\beta_i} = g^{\frac{b}{c}c\beta_i} = g^{r'c\beta_i} = (T_i)^{r'}$ which $r' = b/c$. Accordingly, the cipher-text will be random encryption of the text M_v under the attribute γ_{kp}. In which state the advantage (winning probability) of A as defined is equal to ε, meaning $Pr[v = v'] = \frac{1}{2} + \varepsilon$.

Otherwise, if Z for a random number $z \in Z_p$ is equal to the value $e(g,g)^z$, then $E' = M_v e(g,g)^z$, since Z is a random number, A considers E' as a random element of the group G_2 and includes no information of M_v. In which state, the attacker obtains no information about v, leading to $Pr[v = v'] = \frac{1}{2}$.

Therefore, the probability of the challenger C for solving the problem DMBDH is equal to:

$$\begin{aligned} Adv_c^{DMBDH} &= |pr[C(g, g^a, g^b, g^c, e(g,g)^{ab/c}) | v = v'] \\ &\quad - pr[C(g, g^a, g^b, g^c, Z) | v = v']| \\ &= \frac{1}{2}(\frac{1}{2} + \varepsilon) - \frac{1}{2}.\frac{1}{2} = \frac{\varepsilon}{2}. \end{aligned} \tag{12}$$

5.2 Security proof of the CP-ABE cryptography scheme

The security model of the CP-ABE scheme similar to that of the ID-based cryptography schemes allows the attackers to request the private keys incapable of decrypting the challenge cipher-text. In the following, describing the security game used in Bethencourt et al. to demonstrate the CP-ABE security we show that the CP-ABE scheme used in the MedSBA proposed scheme has proven security in this security model. This game is between a challenger and an attacker, including the following steps:

Setup: The challenger executes the preparation algorithm and sends the public parameters to the attacker.

Phase 1: The attacker requests the private keys for the set of attributes $\gamma_0, \gamma_1, ..., \gamma_m$.

Challenge: The attacker sends two messages M_0 and M_1 of the same-sized lengths to the challenger. Moreover, the attacker announces the access structure $\Gamma^{\star}_{Cp}$ so that none of the attributes sets $\gamma_0, \gamma_1, ..., \gamma_m$ in phase 1 satisfy the access structure $\Gamma^{\star}_{Cp}$. Then the challenger randomly selects a bit b and encrypting the message M_b under the access structure $\Gamma^{\star}_{cp}$ sends the ciphertext to the attacker.

Phase 2: At this phase, phase 1 is repeated provided that none of the attributes sets $\gamma_0, \gamma_1, ..., \gamma_m$ satisfy the structure $\Gamma^{\star}_{cp}$.

Response: The attacker returns a bit b' as the answer. Therefore, the victorious probability of the attacker in this game is equal to:

$$Pr[Bsucceeds] = pr[b = b'] - \frac{1}{2}$$

Similar to all attribute-based encryption schemes, user-collusion is a notable challenge in scheming attribute-based cryptography systems. The private keys in our proposed scheme like that in Sahai and Waters schemes are randomly generated to avoid their sharing, in Bethencourt scheme used in MedSBA scheme secret sharing is included in the ciphertext instead of the private key.

Undoubtedly, the attacker must be able to detect the expression $e(g,g)^{\alpha s}$ to decrypt the ciphertext. To materialize this fact, he should pair the components C of ciphertext and D of user-private key, resulting in the optimal value $e(g,g)^{\alpha s}$ concealed by $e(g,g)^{rs}$. The value $e(g,g)^{\alpha s}$ can only be visible when the user obtains a correct component of the key to satisfy the secret-sharing existing in the ciphertext. Since the concealed value is embedded randomly in the private key of a particular user, collisional attacks will not affect the scheme.

Considering the security model applied in the scheme, the scheme is, undoubtedly, secure facing chosen-plaintext attack and even the security of the scheme encountering the chosen-ciphertext attack can efficiently develop applying random oracle techniques.

5.3 Security analysis of the proposed scheme based on BAN logic

BAN logic has been used to analyze the accuracy of the proposed protocol. BAN logic developed by Burrows et al. (1989) is a logic based on belief and action. A logic that as an official approach depends on the beliefs of the trusted parties involved in the protocol and the promotion of such beliefs over communication procedures to recognize the imperfections of authentication protocols. Table 2 presents the notations used in the BAN logic.

Initial assumptions: The initial assumptions include the initial possessions, ability, and belief of the entities towards the first moment of the protocol as follows:

The initial assumptions associated with the patient P_i:

$$A1.1 : P_i| \equiv |\overset{k_{pub}^{P_i}}{\rightarrow} P_i$$
$$A1.2 : P_i| \equiv \#k_{pub}^{P_i}$$
$$A1.3 : P_i| \equiv \#k_{cp-sym}$$
$$A1.4 : P_i| \equiv U_k| \equiv < \gamma_{cp} >_{SK_i}$$

The initial assumptions associated with the hospital H_j:

$$A2.1 : H_j| \equiv |\overset{k_{pub}^{H_j}}{\rightarrow} H_j$$
$$A2.2 : H_j| \equiv \#k_{pub}^{H_j}$$
$$A2.3 : H_j| \equiv \#k_{kp-sym}$$
$$A2.4 : H_j| \equiv U_k| \equiv < \gamma_{kp} >_{D_j}$$

The initial assumptions associated with the user U_k: U_k is a user who intends to use medical data.

$$A3.1 : U_k| \equiv |\overset{k_{pub}^{U_k}}{\rightarrow} U_k$$
$$A3.2 : U_k| \equiv \#k_{pub}^{U_k}$$
$$A3.3 : U_k| \equiv < \gamma_{cp\ SK_i}$$
$$A3.4 : U_k| \equiv < \gamma_{kp} >_{D_j}$$

The initial assumptions associated with the blockchain nodes:

Table 2 BAN logic notations

Symbol	Description
$P\| \equiv X$	P believes the X statement, i.e. P can decide on the correctness of X
$P \lessdot X$	P sees X, which means it can read and save it
$P\| \sim X$	P once said X statement, i.e. P once said X, and when it says it has believed it
$P\| \Rightarrow X$	P has jurisdiction over in the case of X; that is, if P believes X it is correct
$\#X$	The X statement is fresh, that is, X has never been sent before the run of this step in the protocol
$P \overset{k}{\leftrightarrow} Q$	A common key such as K is shared between P and Q
$\overset{k}{\mapsto} P$	K is the public key P and the corresponding private key is K^{-1}
$\{X\}_k$	The X statement is encrypted with the K key
$\langle X \rangle_Y$	The expression X is combined with the formula Y; this means that Y is a secret, and the presence of that identity expresses the identity of anyone who has declare $\langle X \rangle_Y$
(X, Y)	The formula X or Y is part of the formula (X, Y)

$A4.1 : B| \equiv P_i| \equiv |\overset{k_{pub}^{P_i}}{\rightarrow} P_i$

$A4.2 : B| \equiv H_i| \equiv |\overset{k_{pub}^{H_j}}{\rightarrow} H_j$

$A4.3 : B| \equiv U_k| \equiv |\overset{k_{pub}^{U_k}}{\rightarrow} U_k$

$A4.4 : B| \equiv P_i| \Rightarrow K_{pub}^{P_i}$

$A4.5 : B| \equiv H_j| \Rightarrow K_{pub}^{H_j}$

$A4.6 : B| \equiv U_k| \Rightarrow K_{pub}^{U_k}$

$A4.7 : B| \equiv U_k| \equiv < \gamma_{cp} >_{SK_i}$

$A4.8 : B| \equiv U_k| \equiv < \gamma_{kp} >_{D_j}$

$A4.9 : B| \equiv P_i| \equiv < \gamma_{cp} >_{SK_i}$

$A4.10 : B| \equiv H_j| \equiv < \gamma_{kp} >_{D_j}$

$A4.11 : B| \equiv P_i| \equiv \#K_{pub}^{P_i}$

$A4.12 : B| \equiv H_j| \equiv \#K_{pub}^{H_j}$

$A4.13 : B| \equiv U_k| \equiv \#K_{pub}^{U_k}$

The protocol anticipated goals: The expected objectives include a set of goals that ensure the security of the proposed protocol. The goals include the participating entities believing in the correct execution of the processes in a protocol. Something like believing of the nodes executing consensus on a blockchain in the accuracy of transmitted transactions or the trust of a patient in that only the authorized and his expected entities are capable of decrypting data. Such expected goals are described as follows:

$G_1 : B| \equiv P_i| \sim IT_x$

$G_2 : B| \equiv P_i| \sim PT_x$

$G_3 : B| \equiv H_j| \sim PT_x$

$G_4 : B| \equiv \#(IT_x, PT_x)$

$G_5 : B| \equiv \#IT_x$

$G_6 : U_k \prec\cdot PHI$

$G_7 : U_k| \equiv P_i| \sim IT_x$

$G_8 : U_k| \equiv P_i| \sim PT_x$

$G_9 : U_k| \equiv H_j| \sim PT_x$

The idealization of a protocol flows: Each section of the protocol execution in the idealization of the protocol is modeled based on the BAN logic and a formal definition based on the BAN logic symbolization is provided from the protocol flows.

Data encryption phase by the hospital:

$M(1,1);(P_i \rightarrow B) : B \prec\cdot\prec < IT_x >_{K_{pr}^{P_i}}$

$M(1,2);(H_j \rightarrow C) : C \prec\cdot \{PHI\}_{K_{kp-sym}}$

$M(1,3);(H_j \rightarrow B) : B \prec\cdot\prec < PT_x >_{K_{pr}^{H_j}},$

$B \prec\cdot \{k_{kp-sym}\}_{D_j}$

Data encryption phase by the patient:

$M(2,1);(P_i \rightarrow C) : C \prec\cdot \{PHI\}_{K_{cp-sym}}$

$M(2,2);(P_i \rightarrow B) : B \prec\cdot\prec < IT_x >_{K_{pr}^{P_i}}$

$M(2,3);(P_i \rightarrow B) : B \prec\cdot\prec < PT_x >_{K_{pr}^{p_i}},$

$B \prec\cdot \{k_{cp-sym}\}_{SK_i}$

Data decryption phase:

$M(3,1);(B \rightarrow U_k) : U_k \prec\cdot\prec < IT_x >_{K_{pr}^{P_i}}$

$M(3,2);(U_k \rightarrow B) : B \prec\cdot (< UdT_x >_{K_{pr}^{U_k}}, SC)$

$M(3,3);(B \rightarrow U_k) : U_k \prec\cdot\prec < PT_x >_{K_{pr}^{P_i}}$

or $U_k \prec\cdot\prec < PT_x >_{K_{pr}^{H_j}}$

$M(3,4);(C \rightarrow U_k) : U_k \prec\cdot\prec < PHI >_{K_{kp-sym}}$

or $U_k \prec\cdot\prec < PHI >_{K_{cp-sym}}$

The interpretation of protocol security goals: The protocol security goals are interpreted based on the initial assumptions, protocol flows idealization, and BAN logic standards as follows:

Theorem 1 *The nodes existing on the blockchain network believe that once the patient P_i has generated the transaction IT_x.*

Proof Based on the assumptions $A_{4.1}$ and $A_{4.4}$ and the law $J1$ we have $T1$:

$$(J1) : \frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$$

$$(T1) : \frac{B| \equiv P_i| \Rightarrow K_{pub}^{P_i}, B| \equiv p_i| \equiv |\overset{k_{pub}^{P_i}}{\rightarrow} P_i}{B| \equiv |\overset{k_{pub}^{P_i}}{\rightarrow} P_i}$$

Blockchain network nodes believe $K_{pub}^{p_i}$ is the public key corresponding to the private key $K_{pr}^{p_i}$, and in association with the patient P_i. Thus, based on the message $M(1.1)$ in which blockchain nodes have received a transaction IT_x signed by the private key $K_{pub}^{p_i}$, according to $T1$ result, and rule $RM2$ we have $T2$:

$$(RM2):\ \frac{P|\equiv |\overset{k}{\rightarrow} Q, P\prec\cdot \{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$$

$$(T2):\ \frac{B|\equiv |\overset{k_{pub}^{P_i}}{\rightarrow} P_i, B\prec\cdot \{IT_X\}_{K_{pr}^{P_i}}}{B|\equiv P_i|\sim IT_x}$$

Meaning blockchain nodes believe that once P_i has generated the transaction IT_x, hence, the target G_1 is achieved. Similarly, the targets G_2, G_3, G_7, G_8, and G_9 are proven as well.

Theorem 2 *Blockchain nodes believe the transactions IT_x and PT_x are generated by P_i and based on P_i access structure.*

Proof According to Theorem 1, the blockchain nodes believe the transactions IT_x and PT_x are generated by P_i. Given $A_{4.11}$, blockchain nodes also believe that $K_{pub}^{P_i}$ is fresh. Therefore, according to the rule $F4$ stating if P believes that part of a transposition is fresh, then it will believe that all the transposition is fresh and given $A_{4.4}$ we have:

$$(F4):\ \frac{P|\equiv \#X}{P|\equiv \#<\ X\ >_Y}$$

$$(T3):\ \frac{B|\equiv \#K_{pub}^{P_i}, B|\equiv P_i|\Rightarrow K_{pub}^{P_i}}{B|\equiv \#<\ IT_x\ >_{k_{pr}^{P_i}}, B|\equiv<\ PT_x\ >_{k_{pr}^{P_i}}}$$

Therefore, the target G_5 is proved in accordance with the relation $T4$.

$$(T4):\ \frac{B|\equiv \#<\ IT_x\ >_{k_{pr}^{P_i}}}{B|\equiv \#IT_x}$$

Also, according to the relation $T3$ and the rule $F1$ we have $T5$:

$$(F1):\ \frac{P|\equiv \#X}{P|\equiv \#(X,Y)}$$

$$(T5):\ \frac{B|\equiv \#IT_x}{B|\equiv (IT_x, PT_x)}$$

Similarly, the target $G4$ is proved.

Theorem 3 *The patient P_i ensures the user U_k having appropriate attributes can access the PHI data.*

Proof According to the message $M(3.1)$, the user U_k can receive the transaction IT_x from the blockchain network and the result of the smart contract SC will be valid, in case of having the necessary attributes in the transaction, and receive the transaction PT_x according to the message $M(3.3)$ including the data storage path in the cloud, and K_{kp-sym} or K_{cp-sym} encrypted key information in an encrypted fashion. Therefore, the user U_k can receive the encrypted data from the cloud according to the messages $M(3.3)$ and $M(3.4)$.

$$(T6):\ \frac{U_k\prec\cdot<\ PT_x\ >_{K_{pr}^{P_i}}}{U_k\prec\cdot\{K_{cp-sym}\}_{SK_i}, U_k\prec\cdot\{PHI\}_{K_{cp-sym}}}$$

$$\text{or}\ \frac{U_k\prec\cdot<\ PT_x\ >_{K_{pr}^{H_j}}}{U_k\prec\cdot\{K_{kp-sym}\}_{D_j}, U_k\prec\cdot\{PHI\}_{K_{kp-sym}}}$$

Hence, in accordance with the assumptions $A_{3.3}$ and $A_{3.4}$ and the result T6 we have:

$$(T7):\ \frac{U_k\prec\cdot\{K_{kp-sym}\}_{D_j}, U_k|\equiv<\ \gamma_{kp}\ >_{D_j}}{U_k\prec\cdot K_{kp-sym}}$$

$$(T8):\ \frac{U_k\prec\cdot K_{kp-sym}, U_k\prec\cdot\{PHI\}_{K_{kp-sym}}}{U_k\prec\cdot PHI}$$

Similarly, for the data encrypted by the patient we have:

$$(T9):\ \frac{U_k\prec\cdot\{K_{cp-sym}\}_{SK_i}, U_k|\equiv<\ \gamma_{cp}\ >_{SK_i}}{U_k\prec\cdot K_{kp-sym}}$$

$$(T10):\ \frac{U_k\prec\cdot K_{cp-sym}, U_k\prec\cdot\{PHI\}_{K_{cp-sym}}}{U_k\prec\cdot PHI}$$

Accordingly, the user access to the PHI medical information was materialized meaning G_6 target is proven.

5.4 Comparing security properties

This section presents a comparison between the MedSBA proposed scheme and the recent schemes proposed for sharing from the perspective of the security attributes. Table 3

Table 3 Security properties comparison with the related works

Properties	Yang	Zhang	BBDS	MeDShare	Peterson	BSPP	MedSBA
Blockchain based	×	×	✓	✓	✓	✓	✓
Access control	✓	✓	✓	✓	✓	✓	✓
Immediate accees revocation	×	×	×	×	×	×	✓
Data auditing	✓	✓	✓	✓	×	✓	✓
Privacy preservation	✓	✓	✓	✓	✓	✓	✓
Patient anonymity	✓	×	✓	✓	✓	✓	✓
No online registration center	×	✓	×	×	×	×	✓
Perfect forward secrecy	×	×	×	×	✓	✓	✓

presents the comparison (Yang and Ma 2015; Zhang et al. 2016; Xia et al. 2017a, b; Peterson et al. 2016; Zhang and Lin 2018).

6 Efficiency and simulation

This section evaluates the system efficiency from the viewpoint of computation cost required for the operations of encryption, decryption, and signing transactions and storage space needed on the network for different types of transactions on a blockchain.

6.1 Storage overload analysis of the proposed scheme

Considering the transactions registered on the network include either the encryption key and the PHI information storage path on a blockchain or a description of the PHI information and data access structure on the permissionless blockchain, the size of information stored on the blockchain is of great importance. The amount of information stored on the blocks of a blockchain is dependent on that existing in a transaction. $|G_1|$ and $|G_2|$ are denoted the size of an element in group $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, $|Q|$ the size of an element in $\mathbb{Z}_p$, and t the number of attributes expected for data decryption, the amount of which is equal to m.

Table 4 shows the size of a block and transaction as well, where the block type equal to one byte (permission or premissionless), the block header used to address the block, and the previous hash block size equal to 32 bytes, and each block size 4 bytes are determined. Transaction types (*ITx*, *UdTx* or *PTx*) each is determined by one byte, producer pseudo-identity of each transaction that is equal to $H_3(K^i_{pub})$ by 32 bytes, time stamp by 4 bytes, and ECDSA signature on the elliptic curve secp256 k1 including two components of 32 bytes are identified by 64 bytes per transaction.

The size of the contents of any transaction is different depending on its type; Table 5 has shown that of *ITx*, *UdTx* and *PTx* transactions. As it is observed in Table 5 the size of the contents of the transaction *UdTx* is always constant; however, that of the transactions *ITx* and *PTx* linearly increases depending on the number of system attributes because the size of access structure determined for data decryption linearly increases by increasing the number of attributes required for data decryption. Therefore, increasing the number of attributes required to encrypt data leads to a linear increase in the length of the cipher message. In Table 5, t represents the number of attributes needed to decrypt the data, the maximum value of which will be m. Figure 11 shows the size of each transaction by increasing the expected attributes in the access structure.

6.2 Analyzing the computation cost of the proposed scheme

This section provides an analysis of the computation cost of the key generation, encryption, and decryption algorithms required for the KP-ABE and CP-ABE cryptography used in the MedSBA scheme and the algorithm for producing and verifying digital signatures. Table 6 has provided the computation cost required for the above algorithms. Table 6 ignores the time used for generating random numbers and computing the hash functions against field-based operations such as pairing and power, due to its insignificance. According to Table 6 the computation cost required for key generation, encryption, and decryption of messages, linearly depends on the number of expected attributes t the maximum amount

Table 4 Block storage space for blockchain of the MedSBA scheme

Permission or permissionless block								
Block header				Transaction				
Block type	Block identity	Block size	Previous block hash	Transaction type	Pseudo ID	Payload	Time stamp	Signature
1 byte	32 byte	4 byte	32 byte	1 byte	32 byte	ITx or UdTx or PTx	4 byte	64 byte

Table 5 The storage space required for any transaction of the MedSBA scheme

Payload					
ITx		UdTx	PTx		
PHI descriptor	Γ_{cp} *or* γ_{kp}	Not spent ITx address	ITx address	Path of encrypted data	E_{kp} *or* E_{cp}
512 byte	$t\|Q\|$	32 byte	32 byte	8 byte	(Y_{kp}, E', E_i) $t\|Q\| + \|G_2\| + t\|G_1\|$ or $(\Gamma_{cp}, \tilde{C}, C, C_y, C'_y)$ $t\|Q\| + \|G_2\| + \|Q\| + t\|G_1\| + \|G_1\|$

of which will be equal to m as the maximum number of possible attributes for access to data (Fig. 12).

The number of the group elements in the public parameters of the system in the KP-ABE increases linearly depending on the system attributes (Γ_{kp}). The cryptography algorithm requires $t + 1$ power operations and the maximum of an elliptic curve scalar multiplication operation. The decryption algorithm of KP-ABE requires a power operation and a scalar multiplication at mostly and pairing operations to the number of the considered attributes (Table 7).

The CP-ABE cryptography algorithm requires a power operation for each attribute considered in the access structure Γ_{cp} and the maximum of a pairing operation and a scalar multiplication operation. The key generation algorithm of CP-ABE necessitates two power operations for each user attribute. The CP-ABE decryption algorithm requires at least two pairing operations for each attribute in the access structure Γ_{cp} and the maximum a power operation throughout the path from the leaf node to the root.

The ECDSA signature algorithm demands a scalar multiplication operation and an inverse operation for the signature process, and two scalar multiplication operations and an inverse operation for the process to verify the signature. The process of generating and verifying the signature, regardless of the user's considered attributes, has always consistent computation cost.

Table 7 Symbolization of computation cost

Time complexity of operators
T_{mul} : *scaler multiplication*
T_{exp} : *exponential*
T_{pair} : *pairing*
T_{inv} : *inverse*

6.3 The proposed scheme simulation

Applying OPNET software, this section will simulate the generation, distribution, and registration of medical transactions to evaluate the efficiency of the MedSBA scheme. OPNET software provides a suitable ground for modeling, simulating, and evaluating the efficiency of the networks, and observing the traffic and time of response to the network requests. The OPNET software consists of several distinct editors all controlled by a central editor in a hierarchical manner. The Node editor used for organizing the performance and behavior of nodes, Packet Format editor for determining the type and distribution manner of packets

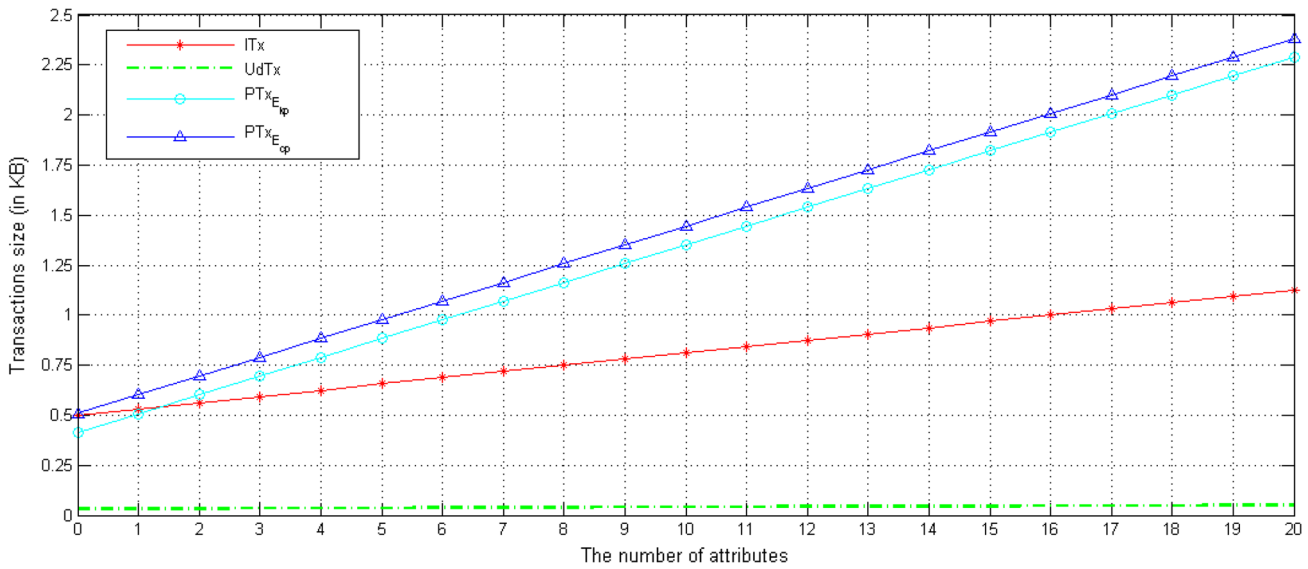

Fig. 12 The size of IT_x, UdT_x and PT_x transactions in the MedSBA scheme based on the expected attributes

Table 6 Computation cost of the MedSBA scheme

	Key generation	Encryption/verification	Decryption/sign
KP-ABE	tT_{exp}	$(t+1)T_{exp} + T_{mul}$	$T_{exp} + T_{mul} + tT_{pair} + T_{inv}$
CP-ABE	$(2t+1)T_{exp}$	$(3+t)T_{exp} + T_{mul} + T_{pair}$	$2tT_{pair} + T_{exp} + T_{inv}$
ECDSA	$2T_{mul}$	$2T_{mul} + T_{inv}$	$T_{mul} + T_{inv}$

on the network, and Process editor for organizing the general behavior of the network, are the significant editors of this software (Cao et al. 2018; Zhu et al. 2002; Salah et al. 2008).

6.3.1 Simulation scenario

Since the OPNET software lacks the cryptography modules simulation, we simulate these modules on the nodes with the characteristics used in the OPNET simulator, applying its influence on the OPNET Node editor (Pournaghi et al. 2018; Bayat et al. 2019a). The time used to execute the cryptography modules of the KP-ABE and CP-ABE depends on the number of anticipated attributes t; therefore, this simulation has considered 5 attributes for each transaction. Table 8 presents the results of the simulation of cryptography modules for $t = 5$ on GMP packets and the two-core Mobile ZM-80 AMD processor. We also run our simulations on Windows 10 at the Core i5 with 3.2 GHz Intel processor and 8 GB RAM. Table 9 shows the size of *ITx*, *UdTx* and *PTx* transactions for $t = 5$ in terms of the byte. Block size is different by the number and type of transactions existing in each block. This simulation has randomly set 25 different transactions in each block.

10 hospitals are simulated in an area of 1500 km^2; each hospital has 10 separate servers called the vdN and bkN nodes having the duty of evaluating the transactions on the blockchain. Each hospital is connected to the Internet by a router, and the servers of each hospital are also linked together in a local area network LAN model by a switch. Therefore, 100 hospital servers in our simulation are linked together in p2p fashion, the task of which is to evaluate the transaction. Figure 13 presents a schematic simulation.

In this simulation, we generate 1000 transactions and distribute them to the network, and then we examine the average transaction time and network traffic load for 24 h. The PBFT consensus algorithm, the time of requests, the process of access to the cloud information, and how to send transactions are simulated using the editors of server nodes and OPNET process.

In this simulation, 10% of the generated transactions are assumed to be invalid; these invalid transactions are distributed based on the Poisson distribution, therefore, the invalid transactions are never confirmed, though leading to increasing the network traffic and response time. Then, in the simulation process, we continue this scenario by increasing the number of network transactions to 1.75 times the initial state and measure network parameters.

Table 8 Time of running the MedSBA encryption modules in mSec

	Key generation	Encryption/ verification	Decryption/sign
KP-ABE	4.135	5.403	45.388
CP-ABE	9.097	15.877	89.047
ECDSA	0.882	1.343	0.461
AES	0.888	0.0011	0.0009

Table 9 Size of transactions in the MedSBA scheme, in bytes

Transaction	Byte
ITx	773
UdTx	133
PTx	1005 or 1101

6.3.2 Simulation results

Figure 14 shows the total number of the transactions distributed in 24 h and that of the valid transactions confirmed on the network. Consequently, about 1000 transactions are transmitted per minute to the network, about 90% of which are trustworthy and about 10% are not validated in the PBFT consensus process.

Also, in Fig. 15, the time of evaluating each transaction on the network is expressed in seconds, as shown in the figure, the average time is about 4.9 s, and this time includes valid and invalid transactions. At any moment of network activity, the validation time of the transactions varies according to the network available resources and the number of valid and invalid transactions, which in our simulation is determined by the poisson distribution. In 24 h of our simulation, this was between 5.2 and 4.6 s, with the average time being around 4.9 s on 24 h.

Figure 16 shows the time of evaluating transactions when the volume of the network transactions has an increase of 75% in comparison to when the network is in normal conditions. In these circumstances, the number of network transactions increases from 1000 transactions per minute to 1750 transactions per minute, while system resources are not added. An increase in the network transactions, initially, makes the evaluation time of each transaction increase about

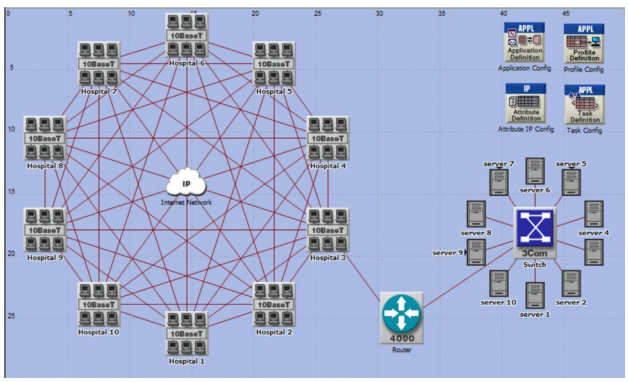

Fig. 13 Schematic Simulation of the MedSBA scheme in OPNET

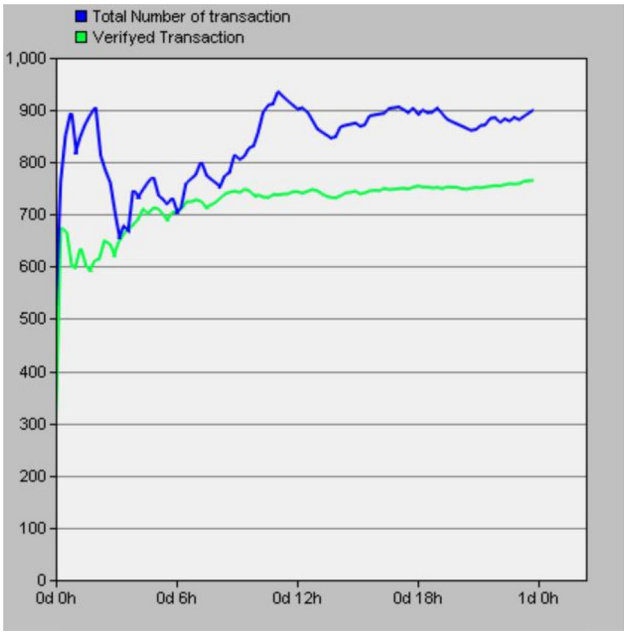

Fig. 14 The total number of network transactions and the transactions confirmed in the MedSBA scheme

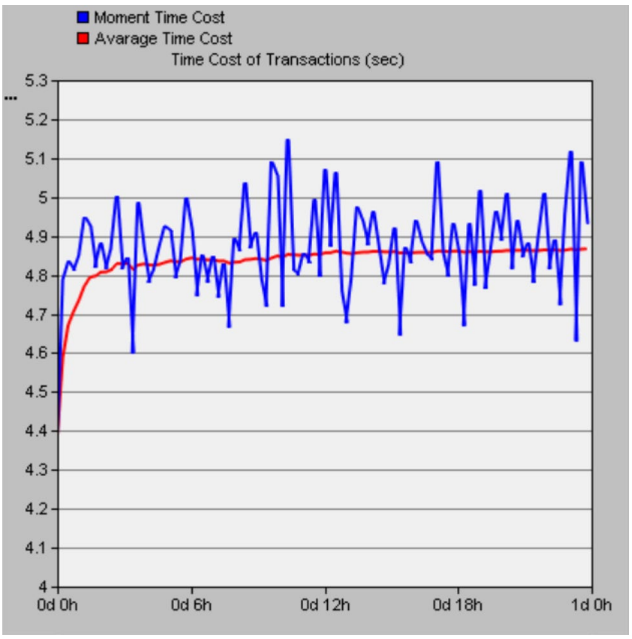

Fig. 15 The average time for each transaction in the MedSBA scheme

7.5 s but after the network gets stability, the evaluation time of each transaction converges to about 6.2 s.

Figure 17 shows the average traffic sent to the network servers in two scenarios of traffic 1 and 1.75 percent in byte per second.

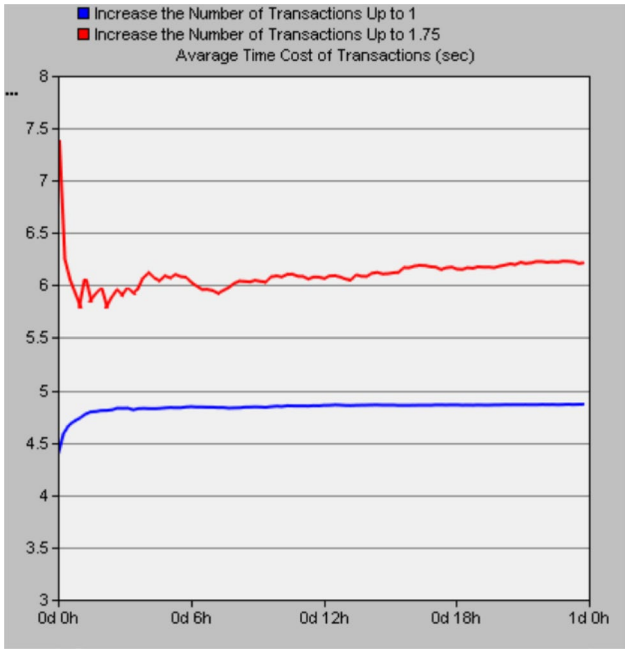

Fig. 16 The average time for evaluating each transaction by a traffic increase of 1.75 times in the MedSBA scheme

Also, Fig. 18 shows the average processing power of the servers 35 and 65% used, respectively, for the two scenarios. Therefore, our simulation results in OPNET show that by increasing network transactions up to 75% without adding system resources used in the network, average network processing increases from 35 to about 65%. Which is very reasonable without increasing network computing resources.

7 Conclusion and future work

The paper has provided a novel and secure protocol to efficiently share medical data between patients, hospitals, and the entities consuming medical data. The proposed protocol includes applying the attribute-based encryption methods combined with blockchain technology. The proposed scheme has applied two attribute-based encryption types KP-ABE and CP-ABE to fine-grain access control of patients on their own medical data and applying blockchain technology has made the network efficiency increase in more effectively transmitting medical data and the methods for instantly revoking the right to access in the attribute-based encryption improve as well. The proposed scheme includes two PBFT consensus-based private blockchains in the permissionless and permissioned forms, the former to distribute the public medical information and the structure for the authorized access to medical data and the latter to set the information of key and storage place on the cloud storing systems. Medical data in our proposed scheme is encrypted using symmetric

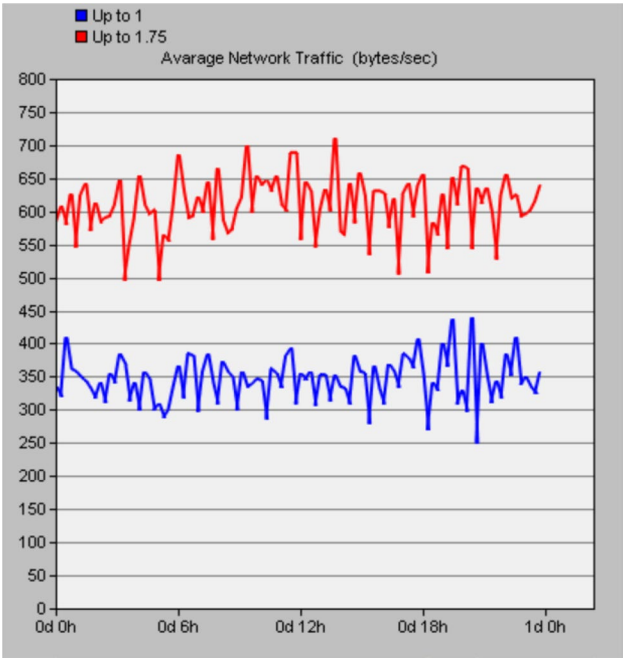

Fig. 17 The average traffic sent to the network servers in two scenarios with the traffic of 1 and 1.75 times in the MedSBA scheme

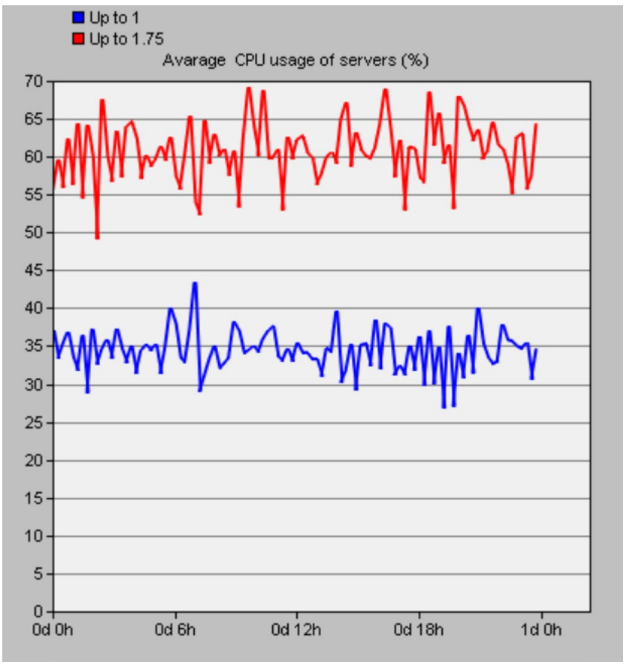

Fig. 18 The average processing power of network servers in the MedSBA scheme

cryptography and randomly stored on the cloud storing systems. Then data cryptography key is encrypted based on the considered access structure by the attribute-based cryptography. Data storage path along with an encrypted key for the information is registered in the transactions of the permissioned private blockchain and a brief description of the data is stored in the transaction of the permissionless private blockchain to be evaluated by the data consumer entities.

We have compared our proposed scheme with other recent ones regarding the security and efficiency attributes and presented time, storage, and computation costs of ours. We have demonstrated the security and appropriate functionality of the proposed MedSBA scheme to achieve the security objectives required for sharing medical data based on BAN logic. We have also verified the security of the KP-ABE and CP-ABE cryptography methods used in our proposed scheme in a formal proof and random oracle model to demonstrate the security of our proposed scheme. Moreover, to investigate the effectiveness of the MedSBA scheme and calculate the delay and traffic load parameters of the network, simulation of this scheme has been evaluated in the OPNET environment, the results of which show the feasibility of our project.

Considering the medical data is valuable to individuals, and many institutions, using medical data, can create added value and earn money, the next step in developing this protocol is to add the possibility of exchanging cryptocurrency between data consumer institutions and individuals to share medical data, So that people make sure they share the benefits of their medical data sharing in a fair way.

References

Aitzhan NZ, Svetinovic D (2016) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Depend Secur Comput 15(5):840–852

Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: using blockchain for medical data access and permission management. In: 2016 2nd international conference on open and big data (OBD). IEEE, New York, pp 25–30

Banerjee M, Lee J, Choo KKR (2018) A blockchain future for internet of things security: a position paper. Digit Commun Netw 4(3):149–160

Bayat M, Barmshoory M, Pournaghi SM, Rahimi M, Farjami Y, Aref MR (2019a) A new and efficient authentication scheme for vehicular ad hoc networks. J Intell Transp Syst. https://doi.org/10.1080/15472450.2019.1625042

Bayat M, Pournaghi M, Rahimi M, Barmshoory M (2019b) Nera: a new and efficient RSU based authentication scheme for VANETs. Wireless Netw. https://doi.org/10.1007/s11276-019-02039-x

Berrut JP, Trefethen LN (2004) Barycentric lagrange interpolation. SIAM Rev 46(3):501–517

Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute-based encryption. In: 2007 IEEE symposium on security and privacy (SP'07). IEEE, New York, pp 321–334

Boneh D, Franklin M (2001) Identity-based encryption from the Weil pairing. In: Annual international cryptology conference. Springer, New York, pp 213–229

Boneh D, Franklin M (2003) Identity-based encryption from the Weil pairing. SIAM J Comput 32(3):586–615
Burrows M, Abadi M, Needham RM (1989) A logic of authentication. Proc R Soc Lond Math Phys Sci 426(1871):233–271
Cachin C (2016) Architecture of the hyper ledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, vol 310, p 4
Cao C, Zuo Y, Zhang F (2018) Research on comprehensive performance simulation of communication IP network based on OPNET. In: 2018 international conference on intelligent transportation big data and smart city (ICITBS). IEEE, New York, pp 195–197
Cartwright Smith L, Gray E, Thorpe JH (2016) Health information ownership: legal theories and policy implications. Vanderbilt J Entertain Technol Law 19:207
Castro M, Liskov B et al (1999) Practical byzantine fault tolerance. OSDI 99:173–186
Dagher GG, Mohler J, Milojkovic M, Marella PB (2018) Ancile: privacy preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:283–297
Deng H, Wu Q, Qin B, Domingo-Ferrer J, Zhang L, Liu J, Shi W (2014) Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Inf Sci 275:370–384
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, American Medical Informatics Association, p 650
Fernndez-Alemn JL, Seor IC, Lozoya PO, Toval A (2013) Security and privacy in electronic health records: a systematic literature review. J Biomed Inform 46(3):541–562
Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security. ACM, New York, pp 89–98
Hamza R, Yan Z, Muhammad K, Bellavista P, Titouna F (2019) A privacy preserving cryptosystem for IoT ehealthcare. Inf Sci 28:17–28
Hankerson D, Menezes A, Vanstone S (2004) Guide to elliptic curve cryptography. Springer, New York
Huang Q, Yang Y, Shen M (2017) Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Gener Comput Syst 72:239–249
Karafiloski E, Mishev A (2017) Blockchain solutions for big data challenges: a literature review. In: IEEE EUROCON 2017—17th international conference on smart technologies. IEEE, New York, pp 763–768
Kaur H, Alam MA, Jameel R, Mourya AK, Chang V (2018) A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. J Med Syst 42(8):156
Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the blockchain model of cryptography and privacy preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP). IEEE, New York, pp 839–858
Kshetri N (2017) Blockchain roles in strengthening cybersecurity and protecting privacy. Telecommun Policy 41(10):1027–1038
Lamport L, Shostak R, Pease M (1982) The byzantine generals problem. ACM Trans Program Lang Syst (TOPLAS) 4(3):382–401
Nakamoto S (2019) Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot
Peterson K, Deeduvanu R, Kanjamala P, Boles K (2016) A blockchain-based approach to health information exchange networks. Proc NIST Workshop Blockchain Healthc 1:1–10
Pournaghi SM, Zahednejad B, Bayat M, Farjami Y (2018) NECPPA: a novel and efficient conditional privacy preserving authentication scheme for vanet. Comput Netw 134:78–92
Riad K, Hamza R, Yan H (2019) Sensitive and energetic iot access control for managing cloud electronic health records. IEEE Access 7:86384–86393
Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, New York, pp 457–473
Salah K, Calyam P, Buhari M (2008) Assessing readiness of IP networks to support desktop video conferencing using OPNET. J Netw Comput Appl 31(4):921–943
Schwartz D, Youngs N, Britto A et al (2014) The ripple protocol consensus algorithm. Ripple Labs Inc White Pap 5:8
Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Workshop on the theory and application of cryptographic techniques. Springer, New York, pp 47–53
Sukhwani H, Martnez JM, Chang X, Trivedi KS, Rindos A (2017) Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: 2017 IEEE 36th symposium on reliable distributed systems (SRDS). IEEE, New York, pp 253–255
Szabo N (1996) Smart contracts: building blocks for digital markets. EXTROPY J Transhumanist Thought (6) 18:2
Tassa T, Dyn N (2009) Multipartite secret sharing by bivariate interpolation. J Cryptol 22(2):227–258
Vahedi E, Bayat M, Pakravan MR, Aref MR (2017) A secure ECC based privacy preserving data aggregation scheme for smart grids. Comput Netw 129:28–36
Wang S, Zhou J, Liu JK, Yu J, Chen J, Xie W (2016) An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Trans Inf Forensics Secur 11(6):1265–1277
Wu HT, Tsai CW (2018) Toward blockchains for health care systems: applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing. IEEE Consum Electron Mag 7(4):65–71
Xia Q, Sifah E, Smahi A, Amofa S, Zhang X (2017a) BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2):44
Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M (2017b) Medshare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5:14757–14767
Yang Y, Ma M (2015) Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. IEEE Trans Inf Forensics Secur 11(4):746–759
Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):218
Zhang A, Lin X (2018) Towards secure and privacy preserving data sharing in e-health systems via consortium blockchain. J Med Syst 42(8):140
Zhang J, Xue N, Huang X (2016) A secure system for pervasive social network-based healthcare. IEEE Access 4:9239–9250
Zheng Y (2011) Privacy-preserving personal health record system using attribute-based encryption. PhD thesis, Worcester Polytechnic Institute
Zhong H, Zhu W, Xu Y, Cui J (2018) Multi authority attribute based encryption access control scheme with policy hidden for cloud storage. Soft Comput 22(1):243–251
Zhu C, Yang OW, Aweya J, Ouellette M, Montuno DY (2002) A comparison of active queue management algorithms using the OPNET modeler. IEEE Commun Mag 40(6):158–167