Secure Cloud-Based Federation for EHR Using Multi-authority ABE

Siddhesh Mhatre and Anant V. Nimkar

Abstract Cloud computing is developed as the most influential perfect models in the IT businesses starting late. Because of the progress implied in cloud computing, it will help data innovation in the healthcare industry. In existing healthcare model, outsourcing storage or accessing record from untrusted cloud servers become a challenging issue for security and privacy of data. An access control model is a productive approach that guarantees the information security in the cloud-based framework. In this work, we present a framework to provide expressive, proficient and revocable healthcare access control for a federation-based model using multi-Authority Ciphertext-Policy based Encryption (CP-ABE) scheme. The existing CP-ABE scheme is not able to fulfil all security need to protect healthcare records and control of privilege revocation problem. This research paper proposes the federation-based multi-Authority CP-ABE (F-CPABE) scheme for healthcare system with its subordinate strategies to outline design to healthcare records in federation-based access control scheme. The attribute revocation technique in this scheme helps to resolve both forward and backward security challenges. It has reduced attribute management overhead from a centralized system and also reduces time complexity.

Keywords Multi-authority · CP-ABE · Access control model
Federation · Electronic health record

1 Introduction

The healthcare organizations have made more than amazing progress from simple paper-based health record to Electronic Medical Records (EMR), from manual surgeries process to robotic surgeries, remote observations for patient and Hospital

S. Mhatre (✉) · A. V. Nimkar
Department of Computer Engineering, Sardar Patel Institute of Technology,
University of Mumbai, Mumbai, India
e-mail: siddhesh_mhatre@spit.ac.in

A. V. Nimkar
e-mail: anantvnimkar@spit.ac.in

C. R. Panigrahi et al. (eds.), *Progress in Advanced Computing and Intelligent Engineering*, Advances in Intelligent Systems and Computing 714,
https://doi.org/10.1007/978-981-13-0224-4_1

Information Systems (HIS), after the involvement of IT in the Healthcare industry [4]. The healthcare records are stored electronically at better places such as with Patient, Medical Practitioners (MPs), Care Delivery Organizations (CDOs) and they are called Patient Healthcare Records (PHR), Electronic Medical Records (EMR), and Electronic Health Records (EHR) respectively [5]. Healthcare organizations are attempting to deal with a different set of the health record [8].

Access control model is a way which provides a guarantee that the records are securely stored at cloud storage with proper access protection [2]. It analyses, evaluates and configures healthcare cloud and services for the secure exchange of EHR. This scheme permits information outsourcing to various cloud suppliers for storing data with the help of access control model in the distributed storage. Ciphertext-Policy based Encryption (CP-ABE) is one of the secure ways for immediate and controlled access to the stored information [7–9]. As the outcome of this research, the proposed framework not just permits EHR information storage but also permits incorporation of various associations and security of records. In existing ABE schemes, as a number of attributes under policy increases size of cipher text becomes very large and overhead on the system increases. The proposed model will help to reduce attribute management from the point of a centralized system and cipher text complexity.

The main contributions of this research can be summarized as follows:

- The proposed model speaks with a various structure of EHRs, for example, drug store, patients, care conveyance association, facility lab, etc.
- This model is used to make unified cloud storage framework in which patients and healthcare members can store and look into own records. They can share records to enhance patient's health by consideration with other healthcare organization.
- This scheme enhances the proficiency of the CP-ABE method by converting the technique into multi-authority CP-ABE. In multi-authority CP-ABE distributed storage framework, client's attributes can be changed intensely on their solicitation. This model provides facilities to a client such as new policies or changes some current ascribes to redesign his consent of information access.

In this research paper, we proposed a new federation-based multi-authority access control model using CP-ABE scheme with detailed construction of the model. Then, we compare proposed the model with existing CP-ABE schemes and results proved that proposed scheme is more efficient than existing CP-ABE schemes. We also mention and resolve both forward and backward security challenges.

The rest of the paper is organized as follows. Section 2 of a literature survey contains a summary and an overview of ABE related work. Section 3 presents our proposed federation-based cloud system with the detailed construction of scheme and Sect. 4 describes framework and assumptions for proposed scheme. Whereas Sect. 5 is focused on implementation and performance analysis of proposed scheme with computation and time complexity. This proposed scheme concluded with a remark in Sect. 6.

2 Literature Survey

There is a vast amount of research done on Access Control models and Attribute-Based Access Control [6]. Yanli et al. [14] describes the framework for encryption and re-encryption using users attributes and attribute group keys in a new scheme called Secure Personal Electronic Medical Record (SPEMR) scheme. It is privileged separation under the multi-owner settings with fine-grained access control. Samydurai et al. [7] describe an access control framework to deal with multi-authority systems with an efficient encryption scheme. It is scalable and dynamic multi-authority scheme. In this scheme, it is difficult to select one access control method to satisfy federation needs [5]. The access control mechanism used in healthcare need to satisfy all participant requirements, i.e. doctors, medical practitioners, patients and medical authorities, etc. to provide secure access to the records. Every member needs to get to specific fields of the health record keeping in mind the end goal to do his employment. To address the above-mentioned issues of access control and compliance management, we present a secure EHRs sharing framework based on multi-authority ABE. This will safely deal with the entrance for composite EHRs coordinated from different medicinal services suppliers at various granularity levels. The proposed scheme also supports Health Insurance Portability and Accountability Act (HIPAA) compliance management to ensure that it satisfies all compliant with HIPAA regulations in clouds.

Attribute-Based Encryption (ABE) is the most common and proficient used cryptographic technique in industry. In this literature, we are concerned about cryptographic enforcement mechanisms for CP-ABE. Sahai et al. [2] introduce the concept of ABE in which an encrypted cipher text is associated with a set of attributes and the private key of the user for an access policy over attributes. The user can only decrypt information if it satisfies the attributes. Sahai et al. [2] present the idea of ABE in which an encrypted information with selected attributes related to the owner and the private key of the owner to create decryption policy for a set of allowed attributes. The user can just unscramble data on the off chance that if it fulfils the properties of policy. Joseph Akinyele et al. [1] improved it by including non-monotonic formula and Goyel et al. [3] improved impressibility of ABE which supports any monotonic formula. To overcome limitations of existing ABE, Wang et al. [11] proposed a multi-authority ABE-based scheme called Multi-Authority based Attribute-Based Encryption (MA-ABE). This is a cloud-based scheme which supports multi authorities to provide access control mechanism with efficient encryption and decryption. In this paper, we work on Yang et al. CP-ABE with multi-authority access control mechanism for the healthcare organization with revocation of authority at any time in the system.

3 Proposed Method for EMR Cloud Federation System Model

The proposed EHR federation manages distinctive elements in various clouds. All health record are made and stored by their own distributed storage in healthcare organization. Cloud Exchange is in charge of the safe trade of the health record inside the cloud federation. There are numerous substances which are needed in health record for the investigation of health status. EHR cloud federation needs access control system which manages retrieval of the health record safely. In the cloud-based storage frameworks, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used for protecting data from unauthorized access with a high level on access security and benefits of the information proprietors more straightforward access strategies [10, 13] (Fig. 1).

The proposed F-CPABE model consist of five elements in the framework: Federation certificate authority (FCA), Attribute authorities (AAs), Cloud Exchange system, Data owners and Data consumers.

- Federation Certificate authority (FCA): This is a globally trusted authority in the federated framework. The FCA initializes the system and permit clients and Attribute authorities (AAs) in the framework. It provides the unique identity to all the elements involved in the federated system. A unique identity is allotted by the Federation certificate authority (FCA) to every single legitimate client in the framework and furthermore, creates the global public key for the clients.

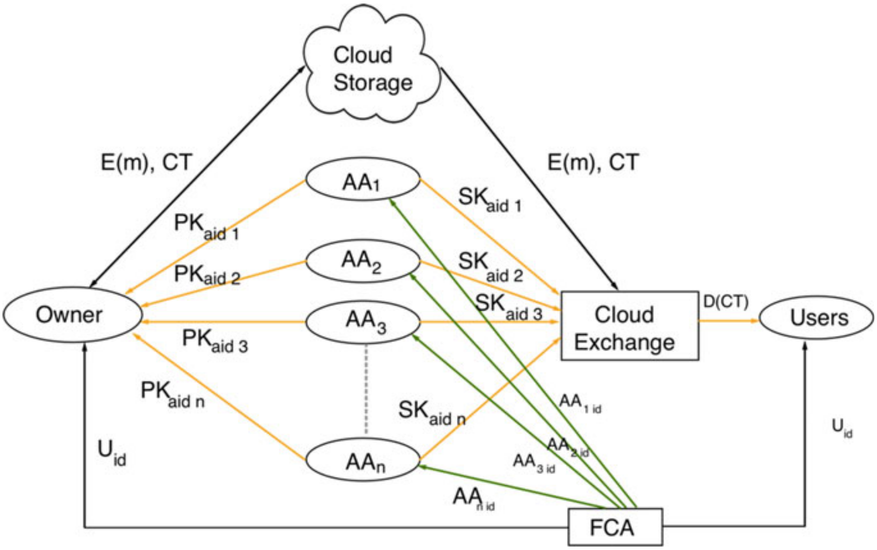

Fig. 1 Federation-based cloud storage system model

FCA also registers Attribute Authorities (AAs) in federation system and generate master public key and master secret key for particular AAs. FCA is not part of in any other quality administration and, the production of client master keys are connected with characteristics of administration.

- Attribute Authorities (AA): It attributes management authority which contains healthcare industries, CDOs, etc. It is responsible for management of users attributes at any time in the system according to their identity or role in its domain. It can add or revoke users attributes at any time in the system. In proposed EHR federation, each attribute assigned by attribute authorities is associated with its respective AA. The same user can have a different set of attributes assign by various AAs. The user does not store attributes as it is taken care by AAs. All the elements come under AA, are managed by attribute authorities, i.e. a number of users, doctors, hospitals, etc. Every AA in EHR federation has full control over the user structure, roles, and semantics of its attributes in the system. Each AAs in EMR federation system generates a local attribute for each user as well as manages revocation and change in the role of the user with reflecting attributes.
- Data Owners: In EHR federation, Data owners can be divided into several components according to the creation of the record. In the health ecosystem, medical practitioner creates EMR record for the patient where medical practitioner with nurse has full access to the health record of the patient. In general, the owner of a health record defines the access policy using attributes from AA or can request attributes from different AAs and encrypt using policies. In EHR federation, we provide multiple ownership for the data which can make changes in records or change in access policy for the record.
- Cloud Storage: Health records made by various participants in the EHR federation for sending encrypted information and receiving information from the server. The cloud server cannot be fully trusted for the information stock-piling and managing its control. This model gives CP-ABE access control system where only the clients who fulfil the attributes are permitted to get the information from EHR federation. All AAs can have their own cloud storage or can share same storage space.
- Cloud exchange: It provides secure record sharing between different AAs without accessing their cloud storage. If AA requires record from other AA, then it can put a request for record sharing to cloud exchange. Cloud exchange gets the data from the AA having the record and gives it to the respective AA.

3.1 Federation Access Control Scheme

To outline the EHR Federation, the most important security issue is to provide attribute revocation for federation-based access control scheme and provide the secure station to information trade in the combined cloud system. However, CP-ABE plan cannot be specifically connected to the federated cloud due to the numerous security issues. In existing scheme, all the encryption and decryption are managed by the central authority where in proposed scheme encryption and decryption are managed by the AAs. Existing healthcare system does not support the revocation of the access to provide security to the health records. A federation-based multi-authority access control model with revocable attributes is been proposed for controlling unauthorized access to healthcare records. This scheme improves the conventional role based model with the new federation-based access control model to work with multiple authorities. It distinguishes the functions of EMR Federation certificate authority (FCA) to the Attribute authorities (AAs). In this FCA acknowledge all the clients in the framework and assign global unique identity (UID) to the client and AAs deal with every property for the client and secret key. In Federation-based access control scheme, secret key allocated by various AAs can be tied together by cloud exchange for decryption of record. Each AAs is associated with an attribute authority identity number (AAID), so in any case, If FCA generates the same attribute for AAs it can be distinguishable.

Whenever EMR cloud-based Federation attribute revocation happens, client or any medical professional and CDOs may upgrade security rule. EHR Federation handles attribute revocation in the framework by controlling every attribute in the system. When revocation happens only components which are associated with the access policy and ciphertext are updated without informing revoked user. All the ciphertexts updating process handled by the server are done in the background and the user need not have to manually update all the ciphertext.

3.2 Attribute Revocation Method

In healthcare system revoking user access is a challenging security issue. The proposed method provides attribute revocation to a limit and stops unauthorized access to the healthcare data. It can be divided into two types:

1. Backward security: The user whose privilege revoked cannot be able to decrypt the updated cipher text.
2. Forward security: Changes in the privilege or new user with sufficient privilege can able to decrypt the previous cipher text using its public attributes.

Access revocation is used for taking away access from selected attribute in EMR federation cloud data. The participant who does not require the access of records any longer can be revoked using this method. At some point in healthcare ecosystem, need for revocation of the access is required. For example, if a patient P_1 visit a hospital H_1 for treatment where he has received treatment from medical practitioners M_1 and M_2, then the health record will be cooperatively created by P_1

and H_1, M_1 and M_2 but after some time if medical practitioners M_2 is not required for the treatment then P_1, H_1 or M_1 can revoke access to medical practitioners M_2. The removed user (whose attribute is revoked) will not be able to decrypt new cipher text because all the attributes policies by them are updated (Backward security).

A new user with sufficient attributes in the system then authorized user or the existing user can also add new user to access control list if he has sufficient permission to add a member. For example, EMR which is encrypted under the policy for H_1 healthcare AND (M_1 Doctor OR N_1 Nurse), which means under the policy M_1 OR N_1 from H1 can be able to decrypt data and they can also add any other doctor to the access control list (forward security).

4 Framework

The Framework setup for the federation-based access control model is as follows:

1. **System Initialization**: It is an initial phase of the system consisting of FCA setup and AA setup. The FCA registers new Attribute Authority (AA) and initializes it. The FCA setup is kept running in the federated framework. It takes attribute information from the user and AAs. For every client and attribute authority, it produces authentication id or user id (UID) as well as creates the unique master public key (MPK) and unique master secret key (MSK) for the certificate. It utilizes the elliptic curve with bilinear maps (or pairings). To introduce a group in the elliptic curve (EC), Two cyclic group of G and G1 created by FCA by using p and q of similar prime ordered group. It additionally picks hash function as shown in Eq. (1).

$$\mathrm{H}\colon \{0,1\}^{*} \rightarrow \mathrm{G}\ \mathrm{and}\ \mathrm{a}, \mathrm{b} \in \mathrm{Zp} \tag{1}$$

For EC with bilinear maps (or pairings), it utilizes symmetric bend with a 512-piece base field. Then FCA generates two random numbers from a set of prime numbers Zp, to generate keys for the registered authority. (1) User Registration to FCA: All the user registrations are performed under the federation rules which is managed by FCA. Every User needs to enrol with own attributes to the FCA for the unique user id. In the enrolment event, if the user is legitimate in the federation framework, the FCA doles out a comprehensively extraordinary unique personality uid to the user. The FCA produces global secret key (SK_{uid}) and the users global public key (PK_{uid}) belongs to every user uid as

$$\mathrm{UserSetup}(\mathrm{U_A}) \rightarrow ((\mathrm{SK_{uid}}, \mathrm{PK_{uid}}), \mathrm{Certificate}(\mathrm{uid})) \tag{2}$$

The FCA additionally produces an endorsement Certificate (Certificate(uid)) for the user uid. At that point, the FCA sends user public key and secret key for the certificate. All keys assign to the user are managed by itself. (2) AA Registration to FCA: Each AA enrols itself to the FCA amid the framework. In this model AAs have a legitimate power in this framework, the FCA first assign a global unique AA identity AA_{aid}. The FCA sends the master secret and public key (MSK_{aid}, MPK_{aid}) to that AA.

$$\mathrm{AASetup}(U_A) \rightarrow ((MSK_{uid}, MPK_{uid}), \mathrm{Certificate}((AA_{uid})) \tag{3}$$

2. **Data Encryption**: The encryption algorithm takes inputs health record (m) data which is hosted on the cloud of different AAs. Data encryption performed for each AAs in the system for all the enrolled user's data. AA uses its public keys MPK_{aid_k} and access policy P of all the involved attributes. Cipher text is denoted as the CT. Encryption is done as in Eq. (4)

$$\mathrm{Ecrypt}(m, MPK_{aid_k}, P) \rightarrow (CT) \tag{4}$$

It isolates the information into a few information segments as $m = \{m_1, m_2, m_3, \ldots, m_4\}$ as indicated by the rational granularities. It scrambles information segments with the policy given to the encryption by utilizing symmetric encryption strategies. It then characterizes structure m_i for every attribute by running the encryption algorithm with policy.

3. **Data Decryption**: All the legitimate clients in the framework can uninhibitedly question any intrigued encoded information. After getting the information from the cloud exchange server, the client uses this algorithm to decode the ciphertext CT by utilizing its global secret keys (SK_{uid}). Once the properties of the client have fulfilled the policy of the cipher text then the only client are liable to decrypt the record.

$$\mathrm{DecryptPHR}(CT, SK_{uid}, A_{uid}) \rightarrow (m) \tag{5}$$

For the EHR records, decryption algorithms run by AAs provides access to the EHR record. AAs take attributes of the user to decrypt data. AAs use its public keys MPK_{aid_k} and access policy P of all the involved attributes. A set of attributes from all the AAs of involved users in the encryption set I_A and Ciphertext (CT). The Decryption algorithm

$$\mathrm{DecryptEHR}(CT, MSK_{aid}, \{A_{aid_k}\}_{aid_k} \in I_A) \rightarrow (m) \tag{6}$$

4. **Cloud Exchange**: Cloud exchange helps to share data from different AAs. Cloud exchange creates the virtual record which will help to share data among

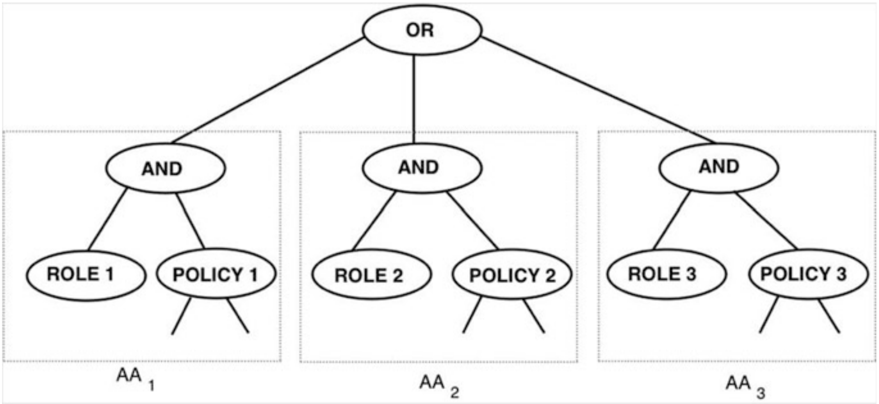

Fig. 2 Access structure for attributes in federation-based cloud system

the different AAs users. If hospital H_1 want to share some records with hospital H_2 then hospital H_1 encrypts data using owners attribute and request for the attributes from the hospital H_2 under AA_2. After getting attributes from AA_2, hospital H_1 of AA_1 encrypts data using OR GATE for with access structure.

Figure 2 demonstrates the multi-authority attribute-based encryption access structure for the share data. In this access structure or Access Tree (AT), four necessities for the model are characterized

- The tree root must be an OR entryway.
- Each offspring of the tree root must be an AND entryway. This must be twofold (binary) gates.
- For every sub-tree of the level 1 AND gates, the right child must be an attribute access policy tree (Policy (K)). This may likewise be an unfilled tree. This tree is named the attribute access policy tree connected with Role K.
- For every sub-tree of the level 1 AND gates, the left child must be a Role quality (Role (K)). This is a leaf. It might be an unfilled tree if and just if the right child of the level 1 AND entryway is avoided tree too. Once access structure is defined its attributes can be used for the encryption of data. All the AA accesses the structure which is defined by the owner of the record to provide access to the other users. Access structure model has two principle points of interest that suit our necessities for the federation-based cloud system which is not optimal in Attribute-Centric ABE model. This model provides auditing efficiency and Policy design flexibility. Other Attribute-Centric ABE Model treats role as a standard property (it is not required to be obligatory). Along with this, there may be an approach that does exclude a role quality, and the reviewing effectiveness of the federation base cloud model is lost.

5 Performance Analysis

To demonstrate the feasibility of proposed approach, we implemented prototype of the federation-based multi-authority CP-ABE model and compared with the existing model of multi-authority CP-ABE proposed by Yang et al. [12]. The F-CPABE model is compared with existing in terms of computation and performance efficiency for encryption and decryption time with consideration of a number of attribute authorities in the federation. It is found that key generation and communication cost is almost similar to the existing models. In EHR federation access control system, only attribute authorities need to store attributes of the user who enrol to the attribute authority. In this model, user and any other authority except attribute authority (AA) store the involved attributes in the system, therefore, storage overhead of the central authority and a user is reduced as compare to the existing model. Attribute authority (AA) is not responsible for managing and storing the public key (PK) or secret key (SK) assign to the owner or users. It will help to reduce storage overhead on Attribute authority. In proposed model, there is no central authority for managing all the attributes and this helps to reduce attribute collusion in the system. In the F-CPABE system, AAs do not communicate with each other. All the communication takes place between AA and cloud exchange, therefore, the communication cost of our access control model is lesser than other models. In this model, communication for the revocation of access and newly added user for authorization is much less because cipher text and policy updates occur only in AAs side unlike other models with the central authority. This helps to reduce overhead from the server to communicate with other AAs. EHR Federation cloud exchange manages all the data sharing from all the AAs so the communication is only with the cloud exchange system which avoids direct access to the cloud storage of other AAs. In other models, for data sharing, all AAs have to share their secret key with each other which can be used for unauthorized access of data.

We achieved federation-based cloud model with a multi-authority CP-ABE scheme on amazon cloud with 3 instances of Ubuntu server with 1 GB RAM and CPU of 2.50 GHz. To implement F-CPABE cloud system, cpabe toolkit [2] with help of other libraries Pairing-Based Cryptography (PBC) to perform mathematical operation of Pairing and charm crypto library for cryptographic operations in the

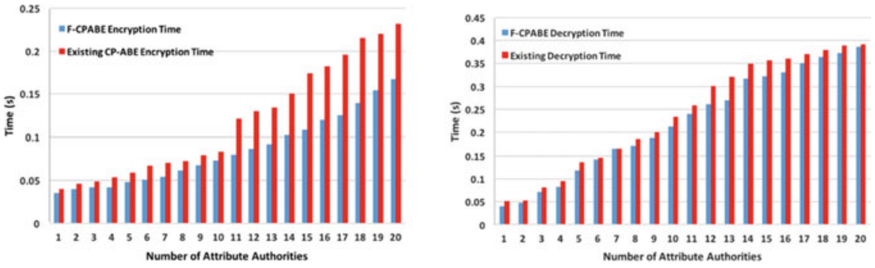

Fig. 3 Performance comparison of F-CPABE with existing multi-authority us CP-ABE

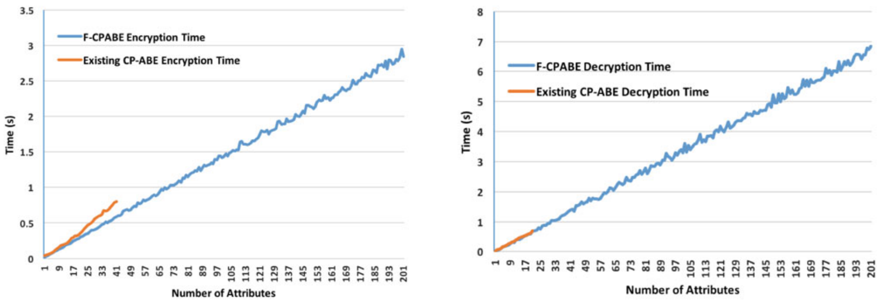

Fig. 4 Time comparison of the of the F-CPABE with existing model

federation base access control model is used. We measure simulation results timings for existing CP-ABE and F-CPABE for the mean of 20 trials for 20 AAs (AA_1, AA_2, …, AA_{20}) with all of the 1 MB file. Figure 3 shows encryption time and decryption time of our model with respect to existing model. It shows that encryption time and decryption time of our model is less than the existing CP-ABE because all encryption and decryption of record are done at AA's side and does not include communication with the centralized server. In this simulation, the encryption and decryption for 200 user attributes (a_1, a_2, …, a_{200}) are carried out and compare with existing scheme. It shows that encryption and decryption performance of F-CPABE is linear with respect to the number of attributes but existing schemes not consistent and it's hard to process when more than 50 attributes are used in existing schemes as shown in Fig. 4 with time utilization. The execution of our scheme is fairly more fascinating. It is marginally harder to gauge without an exact application since simulation timing depends on access policies used in cryptographic operations. The policy tree is randomly generated which is described in Sect. 4 with changing attributes and the size of the policy tree. The trees were produced with beginning from just a root node (OR), then more than once adding a child node to an arbitrarily chosen from different attribute authorities involved in the model. For encryption of data we took random attributes from the attribute authorities involved or have access to health record. Similarly, every running of decryption algorithm we randomly took attributes from attribute authorities who want to access the data and measured the time for the attribute who fulfil the policy structure for the data and excluding the attributes that did not fulfil it.

6 Conclusion

This research used to express two critical security and protection issues in federation-based health care in distributed computing environments: access control on the composite EHRs and HIPAA compliance administration. To address those two issues, a novel framework based on access control policy and logical techniques has been presented. All the more particularly, an EHR information schema approach is proposed to produce composite EHR sharing. In view of the composite EHR information schema, conveyed EHR cases from different healthcare areas can be accumulated into a composite EHR example. Also proposed and illustrated federation-based cloud storage for a healthcare organization by utilizing multi-authority CP-ABE scheme as access control mechanism. The proposed Multi-Authority Attribute-Based Encryption scheme provides an efficient, effective and expressive solution to the health records security problems in sharing health records. It provides revocable solution to the store EHR in the cloud storage. This is more reliable model under some hard cryptographic assumption. This is compared with existing in terms of computation and performance efficiency for encryption and decryption time with consideration of a number of attribute authorities in the federation. We indicated great improvement in encryption and decryption time. It was found that key generation and communication cost is almost similar to the existing models. Our future plan is to implement a model, based on multi-authority attribute-based encryption, to provide the security solution for healthcare data with the real-time application support. The secure trade of information from one cloud supplier to other and furthermore give backing to the Internet of things (IOT).

References

1. Joseph A Akinyele et al. “Securing electronic medical records using attribute-based encryption on mobile devices”. In: Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM. 2011, pp. 75–86.
2. John Bethencourt, Amit Sahai, and Brent Waters. “Ciphertext-policy attribute based encryption”. In: Security and Privacy, 2007. SP’07. IEEE Symposium on. IEEE. 2007, pp. 321–334.
3. Vipul Goyal et al. “Bounded ciphertext policy attribute based encryption”. In: International Colloquium on Automata, Languages, and Programming. Springer. 2008, pp. 579–591.
4. Nimmy John and SanathShenoy. “Health cloud-Healthcare as a service (HaaS)”. In: Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE. 2014, pp. 1963–1966.
5. Anant V Nimkar and Soumya K Ghosh. “An access control model for cloud-based emr federation”. In: International Journal of Trust Management in Computing and Communications 2.4 (2014), pp. 330–352.
6. Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. “DACC: Distributed access control in clouds”. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE. 2011, pp. 91–98.
7. A Samydurai et al. “Secured Health Care Information exchange on cloud using attribute based encryption”. In: Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on. IEEE. 2015, pp. 1–5.
8. Danilo FS Santos, Angelo Perkusich, and Hyggo O Almeida. “Standard-based and distributed health information sharing for mHealth IoT systems”. In: e-Health Networking, Applications and Services (Healthcom), IEEE 16th International Conference on. IEEE. 2014, pp. 94–98.
9. Vijayaraghavan Varadharajan, Alon Amid, and Sudhanshu Rai. “Policy based Role Centric Attribute Based Access Control model Policy RC-ABAC”. In: Computing and Network Communications (CoCoNet), 2015 International Conference on. IEEE. 2015, pp. 427–432.

10. Chang Ji Wang et al. “An efficient cloud-based personal health records system using attribute-based encryption and anonymous multi-receiver identity-based encryption”. In: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on. IEEE. 2014, pp. 74–81.
11. Yun Wang, Dalei Zhang, and Hong Zhong. “Multi-authority based weighted attribute encryption scheme in cloud computing”. In: Natural Computation (ICNC), 2014 10th International Conference on. IEEE. 2014, pp. 1033–1038.
12. Chao-Tung Yang et al. “Implementation of a medical image file accessing system on cloud computing”. In: Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on. IEEE. 2010, pp. 321–326.
13. Kan Yang and Xiaohua Jia. “Expressive, efficient, and revocable data access control for multi-authority cloud storage”. In: IEEE transactions on parallel and distributed systems 25.7 (2014), pp. 1735–1744.
14. Chen Yanli, Song Lingling, and Yang Geng. “Attribute-based access control for multi-authority systems with constant size ciphertext in cloud computing”. In: China Communications 13.2 (2016), pp. 146–162.
15. Hui Zhu et al. “SPEMR: A new secure personal electronic medical record scheme with privilege separation”. In: Communications Workshops (ICC), 2014 IEEE International Conference on. IEEE. 2014, pp. 700–705.