Received: February 3, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Enhanced ABE based Secure Access Control Scheme for E-health Clouds

Padinjappurathu Gopalan Shynu[1]* **Kumaresan John Singh[1]**

[1]*VIT University, Vellore, 632012, India*
* Corresponding author's Email: pgshynu@vit.ac.in

Abstract: The E-health clouds generate an enormous amount of data driven from PHR's, EHR's, EMR's, patient care, compliance and regulatory requirements. To preserve the privacy and confidentiality of the e-health data at untrusted servers various solutions on symmetric key-based access control has aroused. But the major drawback of these techniques is that it is patient centric and do not provide security and fine-grained access control. To solve these issues the paper defines a secure access control scheme for E-health clouds. First, an efficient architecture for E-health clouds is stated and then the access control scheme is defined. As the data stored at the cloud server is highly confidential first a three-factor mutual authentication is made between the cloud server and the data user. Further, the proposed technique makes use of Attribute based searchable encryption with trapdoor function that prevents unauthorised access to the cloud data in an efficient way. The experiment is conducted using charm crypto and the results show that the proposed system provides comparatively better results than the existing techniques.

Keywords: Access control, Attribute based encryption (ABE), Ciphertext policy Attribute based encryption (CP-ABE), Electronic health records (EHR) and personal health records (PHR), Electronic medical records.

1. Introduction

The term E-health defines healthcare practices using electronic processes and communication. E-health clouds are an emerging technique that offers cloud computing services for e-health systems. The application of cloud computing in e-health is widespread as it reduces resource consumption and computational overheads with every individual patient record. In cloud-based e-health systems, the patients' personal health information are examined through a set of body sensors which is projected on, in, or around the patient's body. From the sensor networks, the health information is extracted which includes temperature, blood pressure, pulse and medical images. Once the Patient Health Information (PHI) is collected, it is accumulated into patients mobile devices and then it is further processed and transmitted to the healthcare service providers for distant and exact medical treatment [1]. In such type of systems, an authorised access should be given to the discrete data collected from the patient's mobile devices. Further, the data has to be protected at both the cloud server as well as the data user end with reduced storage and computational overheads. In addition, the health care service providers must fulfil the increasing demands of service consumers who require a higher level of interaction through their computers and low-end computing devices. The data collected from the sensor networks is highly sensitive and it has to be maintained with massive care. As the PHRs plays a vital role in medical diagnosis, only the authorised users should be given the access with distinct access privileges. This creates the need for security, privacy and efficiency over the cloud-based e-health systems.

In the current scenario, hackers are found to be more focused towards stealing sensitive information like medical research records and health information, due to its cost effective nature. Even an outflow of single GB of data may cause a dramatic loss over the medical research analysts and health care organisations. This serious issue of health data outflow not only produces the economic loss, it also leads to greater impacts over the human's life and

medical researchers. This gives rise to the application of cryptographic techniques over cloud-based eHealth systems. At present, the cryptographic techniques such as Role-based access control (RBAC) and Attribute based Encryption (ABE) is prevalent among cloud-based e-health systems [2, 3]. RBAC is the traditional access control model that grants user access provision depending upon the role of the data users. Here the role defines the job functionalities associated with the user [4]. In RBAC the process of selection of appropriate roles and system representation is highly difficult. As the RBAC provides user access, based on the common user attributes like roles, it fails to provide distinct levels of data access privileges among the group of users. This leads to the reduced fine-grained access control properties [5]. Due to these drawbacks, the RBAC techniques are not widely been used among the health care systems [6].

The technique of attribute based encryption was first introduced by Sahai and Waters in the year 2005 [7]. The basic concept behind ABE is that it provides data access provision depending upon the set of attributes possessed by the data users [8, 9]. Key policy attribute based encryption (KP-ABE) and Ciphertext policy attribute based encryption (CP-ABE) are the two major classifications of the attribute based encryption technique [10, 11]. In KP-ABE the data owner defines the data access policies in data users' private key and encrypts the data. The data user can access the data only when the data user attributes satisfies the data owner defined access policies. The major drawback behind the KP-ABE schemes is that the anonymous users obtaining the private key can easily tamper the data [12]. In Ciphertext policy attribute based encryption techniques the data access policy is attached to the encrypted data content. The data user can decrypt the data only when their access policy matches with the data owner defined access policy. In this manner, CP-ABE overcomes the drawback of KP-ABE schemes [13, 14]. CP-ABE is multi-centric in nature as the data content shared by the single data owner can be accessed by the group of users with distinct access policies. Whoever satisfies the data access policies can access the data. This unique property makes it application prevalent among e-health systems [15]. Further in CP-ABE, the level of user access depends on upon the number of attributes possessed by the data users through which it achieves the property of fine-grained access control [15]. In the proposed system the concept of CP-ABE is used.

An application of attribute based encryption in eHealth was given in [16]. This work imposes access control over e-health data using ciphertext policy attribute based encryption technique, where all the users associated with the system can encrypt the data but only an authorised user of a particular domain can decrypt it. Following this work, a self-protecting electronic medical records (EMRs) based on attribute based encryption scheme was given in [17]. In order to deal with the patient privacy and emergency care, this system specifies unique access control policies for every encrypted medical record. Further, it makes use of ABE based access control technique with granular role based and content based access control for EMRs. Thus, it eliminates the need for a single susceptible centralised server. The major contribution of this work is that it provides offline data access through the secure export of EMRs beyond the hospital trust boundary. Another application of ABE in e-health system was given in [18]. It applies Multi-authority ABE technique to E-health clouds, where the PHRs are divided into multiple domains and each authority maintains a particular domain. Further, it applies the technique of attribute based searchable encryption through which the key pairing complexities are reduced. In [21, 22], a precise description of E-health cloud architecture and its working is provided. Depending upon the nature of the EHR the architecture for E-health clouds is divided into two types such as distributed and cloud based architectures. The cloud based architecture consists of the set of remote servers that enables storage and retrieval of the data across the internet. Public, private, hybrid and community cloud are the most widely adopted E-health cloud architectures. The outsourced EHR's are further processed and used for healthcare predictions and research purposes. Cloud assisted wireless body area networks [23] is the most adopted technique for E-health clouds. Through the use of the cloud-assisted wireless body area networks, the EHR's are collected through the base station and are accessed by the end users through the access points. However, the BAN generates an enormous amount of EHR's thus the process of storage and management of the EHR across the cloud computing environment is found to be the challenging factor [24].

Even though there exist several ABE based access control scheme for e-health systems, it does not better suits the needs of security, privacy and efficiency. The major drawback of these techniques is that all these approaches are patient-centric [25]. The patient-centric approaches do not maintain the data collected from the sensor networks in an efficient manner. Further, the access policies associated with such schemes are often complex in

nature [26]. Also, these approaches add extra computational overheads at the client side [27]. As the patient cannot specify and update the data access policies every time. These approaches can lead to data confidentiality issues and it becomes hard to deal with the emergency cases. In addition, the process of user revocation plays an important role in e-health clouds. Whenever the data owner revokes a data user the encrypted data content is downloaded and then data access policies associated with it is modified. This lead to computational overheads and at the same time provision of fine-grained access has become the essential requirement of the e-health clouds. With intent to solve these issues in this paper, we adopt a Health service Provider (HSP) centric approach, where the HSP specifies the data access policies and they take the entire responsibility of patients' health data. Further, we define a trapdoor function through which the data access policies can be modified in an efficient manner without the retrieval of the actual data content. This enables efficient user revocation process and improved security across the proposed system.

Another important issue in E-health clouds is that authenticity of the data users. There is no assurance that the cloud users always communicates with a trusted cloud server. Also, the cloud server is even not aware of the anonymous users. Further, the application of access control techniques is useless if there is no authenticity between the cloud server and the data users. In order to establish a secure communication channel, the process of mutual authentication has become mandatory in e-health applications. Even though there exist several authentication techniques, there is no specific authentication technique that better suits the needs of e-health clouds. As E-health data is highly confidential in nature, an efficient access control and mutual authentication techniques have become mandatory across the e-health clouds.

In this paper, we define a privacy preserving access control technique for e-health clouds that provides a solution to three major issues of e-health systems, such as security, privacy and efficiency of the e-health data. The major contribution of the proposed system is divided into two parts: First, an efficient architecture for E-health clouds is defined. Next, a privacy-preserving access control scheme is given. The proposed system achieves its intended objectives through the implementation of three-factor mutual authentication and Enhanced CP-ABE based attribute searchable encryption techniques.

The proposed architecture makes use of a patient-centric approach that assists in easier handling of the patient's emergency situations. The access control scheme defined in this work; make use of the user biometric identity for the mutual authentication process. First, a three-factor mutual authentication is made between the cloud server and the data users. Upon the successful mutual authentication process, a secure connection is established. Next, a trapdoor function is given to the users. The trapdoor assists in effective user revocation and data retrieval processes. In this manner, the proposed systems provide data access provision across the EHealth clouds.

Three-factor mutual authentication process and the use of trapdoor function with CP-ABE based attribute searchable encryption techniques are the unique functionalities of the proposed system with respect to the existing techniques. The significance of the proposed method is that it reduces the computational complexity and provides improved security and privacy features across the EHealth clouds. The use of biometric features across the three step mutual authentication process provides trusted communication between the cloud server and the data users. Also, the existing EHealth cloud architectures follow the patient's centric approaches where the patient defines the data access policy during the encryption processes. Whereas the proposed system introduces the cloud service provider (CSP) centric approach such that the CSP specifies the access policies and the emergency cases also handled in an effective manner.

The rest of the paper is organised as follows: Section 2 provides a brief description to the proposed system. First, architecture to the E-health systems is given and then the proposed access control scheme for E-Health cloud is discussed in detail. Section 3 describes the significance of the proposed system and section 4, the result analysis of the proposed system. Section 5 provides the conclusion to the proposed system.

2. Proposed System

In this section, we briefly describe the working of the proposed system architecture and its applicability to the E-health clouds.

2.1 System design

The working of the E-health clouds is highly dependent on its underlying architecture. Hence an effective architecture for E-health clouds id defined. An E-health cloud storage system with multiple users and sensitive data are taken into consideration. The proposed system consists of six major entities across a network. An overview of the proposed

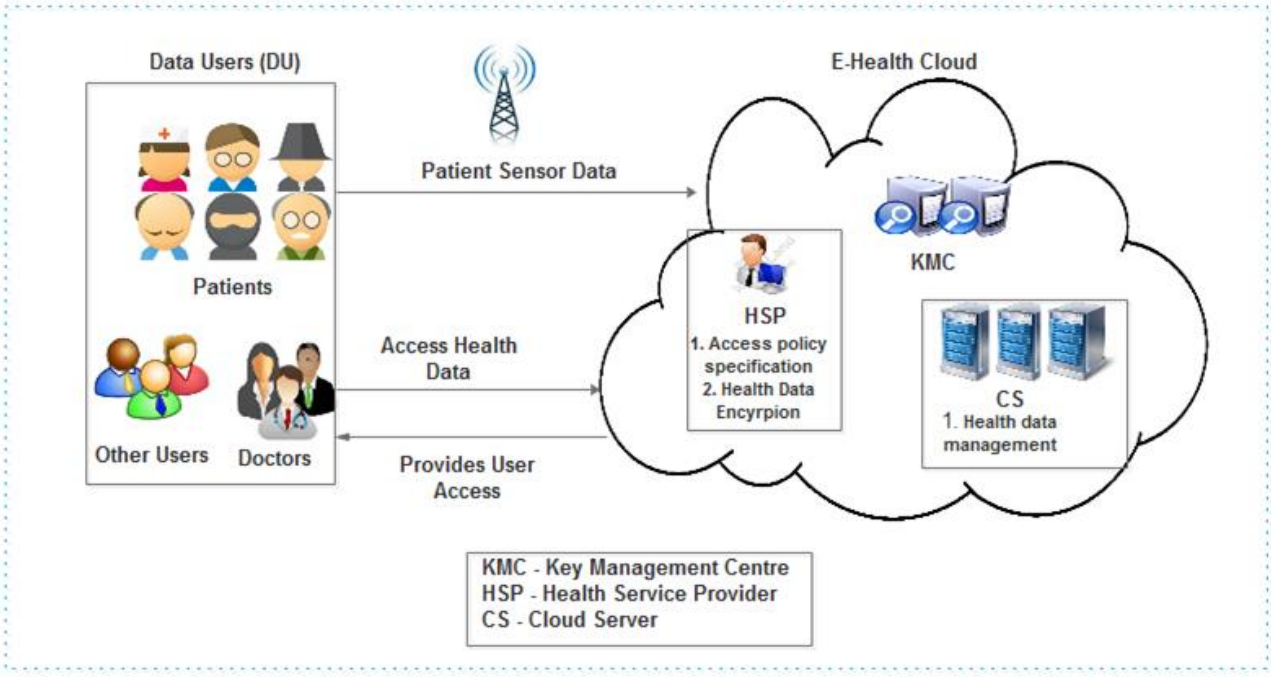


Figure.1 Design of the proposed system

system is described in Fig.1. The working of the system entities are described as follows:

- Cloud server (CS): The cloud server (CS) is a trusted system entity performs all the computational related activities associated with the system. It stores and maintains outsourced patient's sensitive information.
- Key management centre (KMC): The Key management centre (KMC) is responsible for key distribution and management processes. It further distributes attribute certificates to the data users during the mutual authentication process.
- Data owner (DO): The data owner (DO) is a trusted entity share data contents in an encrypted manner and imposes data access policies over the encrypted data. In our case, the Health service provider (HSP) plays the role of the data owner.
- Data Users (DU): The data users (DU) are the users of the data only the authorised user can decrypt the encrypted data content. In our case, the patients, doctors and other data access requester is considered to be the data users.

The proposed system adopts the non-patient centric approach and the Health Service Provider (HSP) plays the role of the data owners. In this architecture patients, health conditions are continuously monitored using sensors networks such as Body Area Networks (BAN). The sensors are projected in and around the patient's body. The BAN networks continuously monitor the patient's health status and collect the health information in the form of Electronic Health Records (EHR). The data collected from the BAN networks are sent to the HSP for further processing. The HSP further analyse and process the patients' health information and stores it over the cloud server in an encrypted manner. Here the HSP is the sole responsibility of the patient's health data. Hence a Service Level Agreement (SLA) is established between the HSP and the data users before they start to communicate with each other.

The first step associated with the proposed system is the user registration process. During this process, the users of the system register with the cloud server and obtain their cryptographic keys. At the end of this process, every data users are given with a public-private key pair and a smart card that contains the set of attributes possessed by them. The next step is the mutual authentication process. That is the secure connection between the data user and HSP takes place only when the HSP trusts the data users' identity and the data user trusts the HSP given attribute certificate. This process is called the mutual authentication process. It takes user's biometric identity, set of public and private key pairs and user's smart card. As a result of this process, the attribute certificate is given to the data users. Next, comes the process of data encryption where the HSP specifies the data access policies (read, write) and performs the process of data encryption. The

proposed system makes use of attribute based searchable encryption technique.

During the process of data encryption, a trapdoor function is calculated for every set of patient's data. The trapdoor acts as a key to the original data and it is derived from the metadata of the original data. Whenever the data access policies associated with the cloud server changes, we do not need to download the encrypted data content to change the access structure instead we can reflect the changes to the trapdoor. The user can decrypt the data only when the HSP defined access policies matches with the attributes of the data user. In this manner, the proposed system provides secure data access across the e-health clouds.

2.2 Working of the proposed architecture

The proposed system consists of the following algorithmic phases:

1. **User Registration process**: During this process, the users of the system register with the cloud server. The user registration process consists of the following algorithmic phases.

Start-up: The start-up algorithm is run by the Key Management Centre (KMC) and takes user security parameter λ as an input and produces master key M_k as output to the data users.

$$Start\_up(\lambda) \rightarrow (M_k) \quad (1)$$

KeyGen: The KeyGen() algorithm generates public and private key pairs to the data users and it is done by the KMC. It takes master key M_k, set of user attributes a_i and the user identity ψ as an input and generates the public and private key pairs to the data users.

$$KegGen(M_k, a_i, \psi_i) \rightarrow (P_k, P_{rk}) \quad (2)$$

At the end of the user registration phase, all users are given a smart card and it is distributed by the KMC. The smart card describes the set of attributes possessed by the data users.

2. **Mutual Authentication Process:** During this process, the data users provides combination of users' biometric identity ψ_i, public key p_k and smart card S as an input to the cloud server (CS). Upon the successful verification of the user credentials the CS generates attribute certificate within the smart card. As a result of the successful completion of the mutual authentication process an attribute certificate is given to the data users. It is given as follows.

$$1)\ A \rightarrow CS: ID_a || ID_B \quad (3)$$

Here in step 1, the data user *A*, initiates the authentication. User *A* issues a request to the cloud server (*CS*) for a session key to protect a logical connection to *B*. The message contains the identities of both *A* and *B* namely, ID_a and ID_B respectively.

$$2)\ CS \rightarrow A : E\left(PK_{cs}, \left[ID_A || PU_a || T\right]\right) || E(PK_{cs}, [ID_B || PU_b || T] \quad (4)$$

Here, the *CS* responds with a message encrypted using private key PK_{cs}. Thus *A* is the only authorised entity which can successfully read the message and A knows that it is originated form the cloud server (*CS*). This message includes a one-time session key PU_a *and* PU_b with a time stamp T for both *A* and *B*. These items are encrypted with PK_{cs} (the master key which is shared to *B*).

$$3)\ A \rightarrow B: E\left(PK_{cs}, \left[ID_A || PU_a || T\right]\right) || E(PK_{cs}, [ID_B || PU_b || T]) || E(PU_b, E(PK_a, [K_s || T])) \quad (5)$$

As shown above, in step 3, *A* stores the session key for future sessions, for reference and it then forward the message $E(PU_b, E(PK_a, [K_s||T])$, which is or iginated at *CS* to *B*. $PU_b$is the information encrypted using the key PK_a and session key K_s with the time stamp *T*.

3. **Encryption:** During this stage, the HSP encrypts the patients' health data and specifies the access policies over it. It takes the message M, public key P_k of the users and the access structure AS as an input and produces the hash message index M_i, trapdoor t_i and the ciphertext CT for the message M as an output.

Let g be the generator and the public key $P_k = g^e$ then the trapdoor function $f(x) = P_k^x$.

The trapdoor t_i is computed as the set of distinct prime numbers of the length k, where $n = p * q$ such that $t_* e = 1 mod\ n$.

Then it is easy to compute $y = f(x)$ and it is difficult to find $y = f^{-1}(x, P_k)$. In this manner the trapdoor function is computed.

The data access policy is encrypted using the ciphertext as $y^d (mod n)$.

$$Encrypt(p_k, A, M) \rightarrow (M_i, t_i, CT) \quad (6)$$

4. **Decryption Retrieve:** During this phase, the user access privileges are verified and their data is retrieved. It is done by the HSP and it takes the set of user attributes a_i, message index M_i, trapdoor t_i and the user access structure as an input and outputs 1 if the M_i matches with the t_i and a_i satisfies AS else it returns 0. The process of data access is given only when the algorithm returns the value of 1 and the user is revoked from the system when the value is 0. Once the user is revoked, they cannot gain access to any of the shared information. The correctness of the trapdoor is verified as $(x^e)^{t_i}(modn) = x^{e*t_i}(modn) = x^1(modn)$.

$$Retrieve(a_i, M_i, t_i) \rightarrow 1 \; or \; 0 \tag{7}$$

5. **Decrypt:** This phase takes the ciphertext CT, set of user attributes a_i and the private key p_{rk} and output the message M only when the set of user attributes a_i matches with the attributes in the data owner defined access structure. It is done by the data users. The trapdoor function is decrypted as $x^e(modn)$.

$$Decrypt(CT, a_i, p_{rk}) \rightarrow (M) \tag{8}$$

This completes the algorithmic processes associated with the proposed technique.

3. Significance of the proposed system

The following are the significance of the proposed technique:

1) Improved security and privacy.
2) The adoption of HSP centric approach and the mutual authentication processes results in improved security measures.
3) Reduced computational overheads. The implementation of trapdoor function reduces the complexity measures associated with user revocation processes.
4) Further, the proposed system offers improved fine-grained access control properties to the data users.

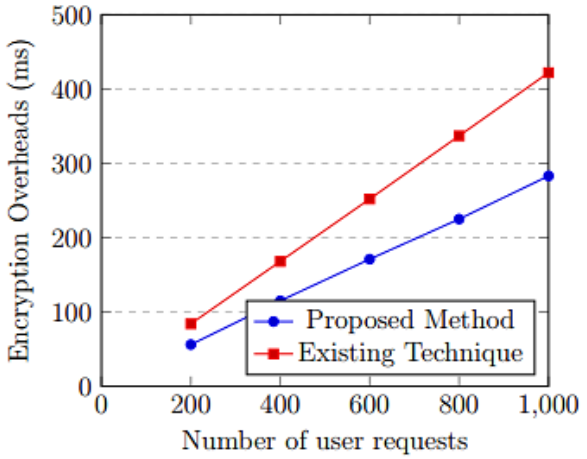
4. Results and discussion

CP-ABE offers fine-grained access control but it leads to increased computational overheads. As the working of the CP-ABE technique is completely dependent on the data access policies, the complex data access policies result in increased computational overheads. In simple terms, the time taken for encryption and decryption process is completely dependent on the data access policies. Further, the complexity of the data increases with the sensitivity of the data contents. This creates composite data access policies across E-health applications. The overheads do not only include the encryption and decryption processes it also results in concurrent key updates and user revocation processes. However, the proposed technique overcomes these drawbacks through the implementation of the appropriate techniques and the performance of the proposed solution is evaluated and compared with the existing techniques. The proposed system was implemented using charm crypto [28], a rapid prototyping technique for cryptographic systems. The experimental set up is created using Ubuntu 14.04 LTS 64 bit system at our home institution in the presence of an ambient induced load. The configuration of hardware components includes Intel Xenon 3.2GHz processor, 3GB RAM and 40 GB available of single SCSI drive. Charm implementation requires dependencies such c math libraries, GNU Multi-precision Arithmetic Library, Pairing-Based Cryptography, OpenSSL and Python 3.2. In order to implement the proposed algorithm, the above-mentioned dependencies are installed and executed. Further 224-bit elliptic MNT curve is used in specific. Charm provides and extensible framework that supports the development of advanced cryptographic schemes and protocols. The results of the proposed techniques were compared with the existing techniques [10]. The experiment is conducted with the dataset taken from [29], which contains biometric identities of the data users through which the genuine cryptographic keys are generated.

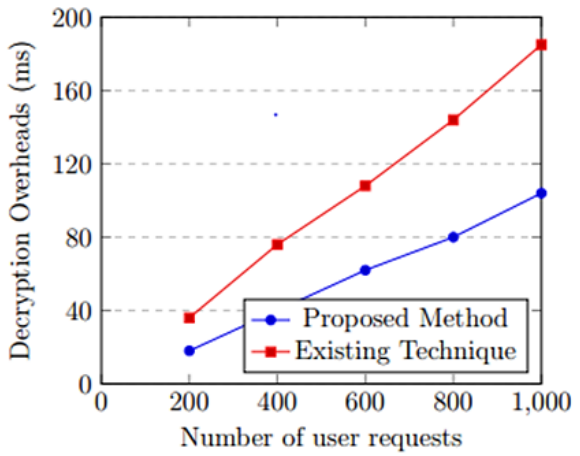
To evaluate the performance of the proposed system, simulations are made several times with distinct type of user requests. A combination of data encryption, read and write access requests are given simultaneously from distinct user nodes. An average computational time measure was calculated for every 100 user requests.

First, the experiment was conducted to measure the computational overheads associated with the encryption process. The computational overhead is measured in time (in milliseconds) and it describes the excess or additional computational time. During the encryption process, the data is encrypted by the HSP and it is shared among the authorised data users. The HSP imposes the data access rights through the specification of data access policies. It has been observed from the experiment (Fig. 2 (a)) that the average computational overhead for the encryption process is 28ms. The encryption overhead with the existing technique is found to be

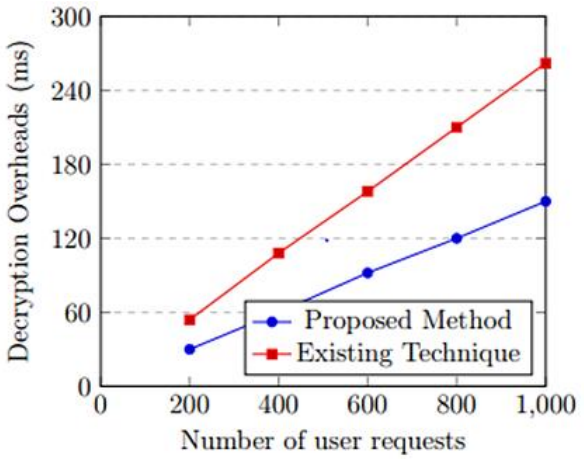
39ms. This is comparatively higher than the proposed system. The computational overhead for the data encryption process includes the time taken to specify the data access policies and to perform the encryption processes.



(a)



(b)



(c)

Figure.2 Simulated results: (a) computational overhead analysis, (b) simple data access policy, and (c) complex data access policy

Table 1. Complexity measure comparison

Time Complexity Comparison		
Technique	**Algorithm**	**Computational Time**
Existing Method	Start-UP	$O(n^3)$
	KeyGen	O(n)
	Encryption	O(2n)
	Decryption	$O(nx(n+1))$
Proposed Method	Start-UP	O(n)
	KeyGen	O(n)
	Encryption	O(1)mod
	Decryption	2n+3

Next, the simulation is made to find the computational measure associated with the decryption process. First, the simulation is done with simple data access policies as in Fig. 2 (b). The results are analysed and the proposed system shows an overhead of 10ms and the existing techniques with the overhead of 21ms of time. Next, the same simulation is repeated with complex data access policies. The result shows that the proposed system takes a minimum overhead of 15.61 ms, whereas the existing technique shows 28.1ms. Thus the proposed technique is more efficient than the existing scheme (Fig. 2 (c)).

The variation in computational overheads is due to the complex data access policies. The proposed technique deals with complex data access policies through the use of attribute-based searchable encryption techniques and trapdoor functions. Through which it easily retrieves the data contents. Further, the trapdoor functions assist in efficient revocation processes. This describes the improved the security and privacy measures of the proposed technique. In addition, the overall complexity measure of the proposed and the existing scheme is described in Table 1.

It has been concluded from the above observation that proposed technique provides improved performance measure compared to the existing e-health cloud schemes. The reason is that it makes use of the attribute based searchable encryption technique with trapdoor functions which enables efficient retrieval of patient's health data. It updates data access policies without the retrieval of the file content. This improves the performance of the proposed system. Further, the mutual authentication processes associated with the proposed technique improves the security measures of the system. In this manner, the proposed technique better solves the drawbacks of the existing e-health clouds. Thus the major advantage of the proposed scheme is that it provides reduced

complexity with improved privacy and security measures.

5. Conclusion

In this paper, we addressed the challenge of fine-grained access control and user's data access security and privacy in e-health clouds. To achieve this objective, we proposed a secure and efficient architecture. First, a three-factor mutual authentication scheme is made between the cloud server and the data users, through which the authenticity of the sensitive patient's health data is preserved. Next, an ABE-based efficient access control scheme was implemented by enhancing the CP-ABE scheme, by which the computation overhead is reduced and improved the privacy of PHR data stored in the Cloud servers. The proposed system make use of a trapdoor function which updates the data access policies without the retrieval of the file contents from the cloud server which enables easy revocation of users. In future, this work can be extended to provide a more efficient ABE-based data access control in e-health Clouds.

References

[1] X. Jin, R. Krishnan, and R. Sandhu. "A unified attribute-based access control model covering DAC, MAC and RBAC", In: *Proc. of the IFIP Annual Conf. On Data and Applications Security and Privacy*, Springer Berlin Heidelberg, pp.41-55, 2012.

[2] N. Shrestha, A. Alsadoon, P. Prasad, L. Hourany, and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system", In: *Proc. of Sixth International Conf. On Digital Information Processing and Communications (ICDIPC)*, pp.75–79, 2016.

[3] L. Ibraimi, M. Asim, and M. Petković, "Secure management of personal health records by applying attribute-based encryption", In: *Proc. of Sixth International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth)*, pp.71-74, 2009.

[4] P. G. Shynu, and K. J. Singh, "A Comprehensive Survey and Analysis on Access Control Schemes in Cloud Environment", *Cybernetics and Information Technologies*, Vol.16, No.1, pp.19-38, 2016.

[5] A. Abbas and S. U. Khan, "A review on the state of-the-art privacy-preserving approaches in the ehealth clouds*"*, *Journal of Biomedical and Health Informatics*, Vol.18, No.4, pp.1431–1441, 2014.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proc. of the 13th ACM Conf. on Computer and Communications Security, pp*.89-98, 2006.

[7] N. Attrapadung, B. Libert, and E. Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertext", In: *Proc. of International Workshop on Public Key Cryptography",* Springer Berlin Heidelberg, pp.90-108, 2011.

[8] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts", *Theoretical Computer Science*, Vol.422, pp.15-38, 2012.

[9] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing", International *Journal of Security and Networks*, Vol.6, No.2-3, pp.67-76, 2011.

[10] L. Zhang, Q. Wu, Y. Mu, and J. Zhang, "Privacy-Preserving and Secure Sharing of PHR in the Cloud", *Journal of medical systems*, Vol. 40, No. 12, pp.267-278, 2016.

[11] P. G. Shynu, and K. J. Singh, "An Enhanced CP-ABE Based Access Control Algorithm for Point to Multi-Point Communication in Cloud Computing", *Journal of Information Science and Engineering*, Vol.33,No.3,pp.837-858, 2017.

[12] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption", In: *Proc. of 35th International Colloquium on Automata, languages and programming*, Reykjavik, Iceland, pp.579-591, 2008.

[13] C. C. Lee, P. S. Chung, and M. S. Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments." *IJ Network Security*, Vol.15, No.4, pp.231-240, 2013.

[14] A. Lewko, O. Tatsuaki, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption", In: *Proc. of the* Annual *International Conf. On the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, pp.62-91, 2010.

[15] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-

based encryption", *IEEE transactions on parallel and distributed systems*, Vol.24, No.1, pp.131-143, 2013.

[16] Y. Li, L. Guo, C. Wu, C. H. Lee, and Y. Guo, "Building a cloud-based platform for personal health sensor data management." In: *Proc. of International Conf. On Biomedical and Health Informatics (BHI), IEEE-EMBS*, pp.223-226, 2014.

[17] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures", IEEE *Transactions on Information Forensics and Security*, Vol.8, No.1, pp.76-88, 2013.

[18] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, N. J. Zachary, and A. D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption", In: *Proc. of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pp.75-86, 2010.

[19] S. Ruj, "Attribute based access control in clouds: A survey", In: *Proc. of International Conf. On Signal Processing and Communications (SPCOM)*, IEEE, pp.1-6, 2014.

[20] A. Sahai, and B. Waters, "Fuzzy identity-based encryption", In: *Proc. of* Annual *International Conf. On the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, pp.457-473, 2005.

[21] N. M. Shrestha, P. W. C. Prasad, L. Hourany, and A. Elchouemi, "Enhanced e-health framework for security and privacy in healthcare system", In: *Proc. of Sixth International Conf. On Digital Information Processing and Communications (ICDIPC), IEEE*, pp.75-79, 2016.

[22] Y. Tong, J. Sun, S. S. Chow, and P. Li, "Cloud-assisted mobile-access of health data with privacy and auditability", IEEE *Journal of Biomedical and Health Informatics*, Vol.18, No. 2 pp.419-429, 2014.

[23] H. Yang, and V. Oleshchuk, "Attribute-based authentication schemes: a survey", *International Journal of Computing*, *Vol.* 14, No. 2, pp. 86-96, 2015.

[24] P. Yang, M. I. Gofman, S. D. Stoller, and Z. Yang, "Policy analysis for administrative role based access control without separate administration", *Journal of Computer Security*, Vol.23, No. 1, pp.1-29, 2015.

[25] Y. Buket, K. Alptekin Ö. Özkasap, "Research issues for privacy and security of electronic health services", Future *Generation Computer Systems*, Vol. 68, pp. 1-13, 2017.

[26] Y. Zhang, Q. Meikang, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data", *IEEE Systems Journal*, Vol.11, No.1, pp.88-95, 2015.

[27] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage", *IEEE transactions on information forensics and security*, Vol.8, No. 12, pp. 1947-1960, 2013.

[28] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems", *Journal of Cryptographic Engineering*, Vol.3, No. 2 pp.111-128, 2013.

[29] Datasets on biometric identities fvc 2000, http://bias.csr.unibo.it/fvc2000/db1.asp, Accessed: 2016-10-12.