Gazi University Journal of Science
GU J Sci
29(3):583-591(2016)

Enhanced Secure Sharing of Personal Health Records in Cloud Computing

R.KALAISELVI[1,♠], K.KOUSALYA[2], R.VARSHAA[3], M.SUGANYA[3]

[1]*Assistant Prof., Dept. of Computer Science and Engineering, Kumaraguru College of Technology , Coimbatore-641049,Tamilnadu,India*
[2] *Professor, Kongu Engineering College*
[3] *Kumaraguru College of Technology*

Received:11/05/2016 Revised:18/06/2016 Accepted: 05/08/2016

ABSTRACT

Personal Health Record (PHR) is an electronic application used by patients to maintain and manage their health information in a private, secure and confidential environment. In cloud computing, cloud providers act as a third party for the information exchange of personal health records. Though this technology facilitates efficient management and the sharing of patient's personal health record, there are wide privacy concerns such as the exposure and accessibility of sensitive health information by unauthorized users. In order to provide security and privacy, it is necessary to encrypt the data before outsourcing and only authorized users with valid attributes must be allowed to access the data. Hiding the users' information is also important while accessing data over the network. Moreover to reduce the key management complexity of data owners, personal health records are classified into multiple security domains. To hide the user information, anonymous authentication through Attribute-Based Encryption (ABE) technique and fine-grained data access control through AES are adopted. This combination provides a high degree of privacy and security for the PHR file. This scheme enables the dynamic modification of access policies or file attributes and on-demand user revocation. Extensive experimental and performance analysis show that the proposed scheme is efficient in terms of security and privacy.

Keywords: *Attribute Based Encryption (ABE), Personal Health record (PHR), anonymous authentication, Advanced Encryption Standard (AES).*

1. INTRODUCTION

Cloud computing is an emerging technology where all the IT resources are provided as services via internet. Major Service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) that decorate cloud, all of which mean a Service Oriented Architecture (SOA) [1]. Cloud services are been adopted widely due to its cost effectiveness and scalable service delivery platform.

♠Corresponding author, e-mail: *kalaiselvi.r.cse@kct.ac.in*

In recent years, Personal Health Records have developed as the emerging trend in the health care technology. Cloud environment allows a patient to create, manage, and control his/her personal health data from anywhere through the web, which has made the storage, retrieval and sharing of the medical information more efficient. Especially, each patient is promised a full control over their medical records. A patient can share their details among wide range of users, including healthcare providers, family members or friends based on their needs or willingness. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks in cloud environment. Due to the high cost of building and maintaining specialized data centers, many health record services are outsourced to or provided by third-party service providers, for example, Google drive, iCloud and Dropbox [2]. Generally, cryptography based encryption and decryption methods are used for security [3].

RSA algorithm can be used to encrypt the data before it is outsourced in the cloud. Here to recover the data, a user must request the key manager to generate the public key provided that the user must be an authorized person [4]. Previous researches on security reveal that, to ensure security in cloud three protection schemes: Hash generation algorithm, Captcha algorithm and AES algorithm have been widely used [5]. Currently, digital signature is used for authentication and AES encryption algorithm for data confidentiality [6].

The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. The PHR system has the ability to limit the access control of users to the application. To achieve this, the access policies are made associate with the various set of user attribute. To improve upon this concern, data is encrypted under a set of attributes so that multiple users who possess proper keys only can access the data [7]. This potentiality leads for an efficient encryption and key management. A secure multi owner scheme can also be imposed in the multi access network where the data can be shared securely in the untrusted cloud [8].

As Attribute Based Encryption (ABE) has the unique feature of preventing user collusion to a significant level to achieve fine-grained access control, a Cipher text Attribute Based Encryption (CP-ABE) is used [9]. Attribute-based encryption (ABE) is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes [10]. Generally search over encrypted documents is a difficult, time consuming process where machine coded genetic optimization algorithms can be employed to reduce the overhead [11].

Thus, these are some of the implementations which secure the cloud related data and several researchers are contributing towards cloud security, still usage of encryption techniques on cloud needs certain improvements.

2. EXISTING SYSTEM

Several security schemes are under practice for knowledge sharing on untrusted servers. Those approaches allow data owners to store the encrypted files in untrusted storage and distribute the corresponding decoding keys solely to the authorized users. Thus it is believed that unauthorized users cannot learn the information files stored on the servers. In these models AES is employed as the chief encryption primitive.

SriVarsha et al., proposed an encryption technique which uses the substitution and permutation method. Here the key idea is arranging the data based on attributes which facilitate access control and AES for securing the records [10].

Randeep Kaur et al., analyzed cloud security algorithms and had a study on comparison of symmetric algorithms on the basis of different parameters. Their experimental results show that AES is faster and secure algorithm [12]. AES has been implemented widely in many platforms and it is tested for many security applications.

Shaik Hussain et al., tried to revoke the access permission of the user using two techniques namely ABE and Proxy Re Encryption (PRE) in p2p cloud storage. This makes the data secure on the cloud. Existing techniques are expensive in terms of time and efficiency when compare to AES [13].

Vikas Vitthal Lonare et al., have proposed a technique Secure Hash Algorithm (SHA) for efficient authentication where the file is encrypted using AES to ensure distributed accountability. The sender hashes the file and sent to the recipient. The recipient then hashes the received file and then checks for the hashes match [14]. As SHA supporting in producing a longer hash value and it is more collision resistant, it is used in widespread.

Jasim et al., analyzed the performance of encrypted database and concluded that the performance of encrypting large database using asymmetric-key algorithm is lower when compared to symmetric-key algorithm [15]. Hence asymmetric-key algorithms can be used for encrypting short key value.

Generally, log files record the access details of the data user. Since the log files are not encrypted, the privacy is not preserved. As this reveals the user anonymous details, there is no security for health records. This leads to wrong authentication and data insecurity.

Mainly SHA is used for authentication as it preserves data consistency and semantic values of entities after hashing.

Though it is widely used, it provides only a one-way hash. So it cannot support encryption and decryption of data over storage. Moreover this algorithm is slower computational algorithm and has known security vulnerabilities.

In few systems like health records management a central authority (CA) has been appointed to perform key management of professional users. But that again requires too much trust on single authority. Single authority may suffer from key over encrypted data. Hence it is advantages of using new encryption pattern called Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism.

As many researchers analyzed various algorithms and combinations of different techniques on data security in cloud environment, a suitable combination of algorithms for authentication and authorization may help in efficient scalable secure data storage.

3. OUR CONTRIBUTION

Health records are maintained in the distributed environment. To assure the patient's control access over their own PHRs, one of the promising methods is encrypting the PHRs before outsourcing. To assure the data security ABE scheme is used.

As there is a possibility for intruders to smell the signature of authorized users, sensitive data stored in remote servers may be misused. In many systems, an implicit assumption underlying is that each user has some unique identifying information associated with them which they can use to prove who they are. As many authentication protocols are simple, the communication can be easily hijacked and details can often be accessed wirelessly without awareness of the owner. To prevent the malicious users, anonymous authentication can be encouraged using the constructive cryptography framework. To achieve this, ABE technique is leveraged to encrypt user authentication details. As of our detailed study ABE was not yet employed for authentication. But our experimental analysis proved that ABE supports an efficient anonymous authentication.

Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share their PHR among a set of users by encrypting the file under a set of attributes, without the need of knowing complete list of users.The encryption and decryption process will be done using Advanced Encryption Standard. AES is employed as the chief encryption primitive. The encryption is done in specified number of rounds. This makes the data more secure.

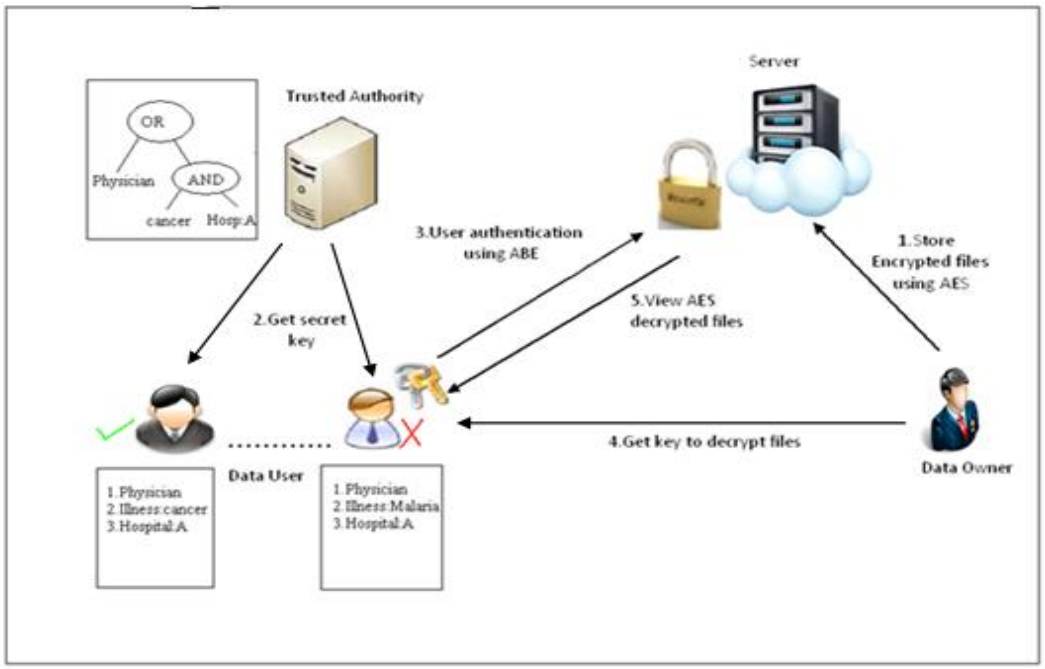

Fig.1 Architecture of user anonymous authentication system

3.1 System Description

This section, describes the architecture of user anonymous authentication system as shown in Fig 1 which consists of three entities:

Cloud service provider: This provides data storage and retrieval service to the subscribing users where data owner stores their data in encrypted format. Only the authorized user can retrieve the encrypted data from the storage and then data is decrypted in the client side by getting appropriate decryption key from the data owner.

We assume that the cloud service provider is semi-trusted, that means that it follows the protocol specified in the system. However, it is assumed that it seeks to learn the information in the encrypted content during the query and response processes as much as possible with malicious intent. In the proposed scheme, the decryption key is directly forwarded to user, where service providers cannot interfere in transferring decryption key to user.

Trusted authority: Authentication of user is done by receiving appropriate attributes and authentication key where key is generated by trusted authority which resides in server. It generates public parameters and the master secret key, which are the primary key materials for the entire process of the proposed scheme. It also generates user-specific private keys which correspond to the set of attributes for data access, cipher text decryption, and anonymous keys for receivers.

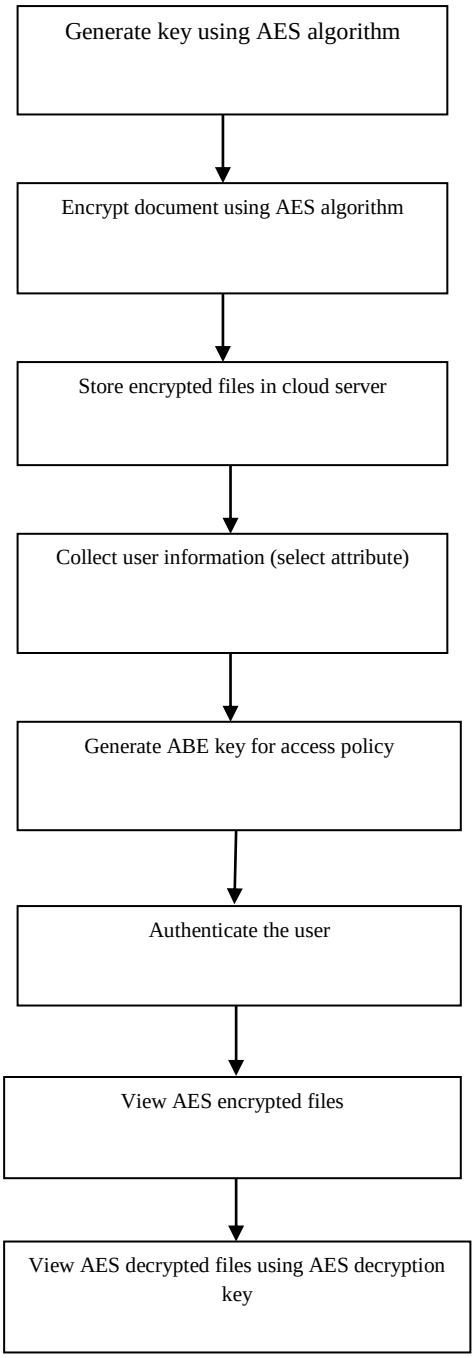

Fig. 2 Process of Encrypted Data storage and Retrieval

Data owner: This is the cloud storage subscriber who wants to upload their data content to the cloud storage system after encryption. The encrypted content can be shared with intended receivers who have sufficient credentials. The Patients can access the records whenever and wherever required. The authentication principle achieved to access the health record based on the permission granted. Here multiple data owner scenario is proposed to manage the health record in sensitive manner. A key management paradigm is proposed to achieve the encryption over the attributes. Complexity is increased between owners and the end users. The access permission is denied from different user regarding medical records for various purposes. Fig 2. describes the process of encrypted data storage and retrieval.

3.2 Proposed Framework

The main goal of this framework is to provide secure patient-centric PHR access and efficient key management. The key idea is to divide the system into multiple security domains such as public and private according to the different user's data access requirements. The personal health record consists of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a health can be mapped to an independent sector in the society, such as the health care, government or insurance sector. The different users make accesses to PHRs based on access rights assigned by the owner.

Few previous researchers have employed SHA for authentication, but it cannot assure the security at high level. In the PHR accessibility, the authorization of health record ensures high level of security. After uploading the health record into the server, the owner retrieves the key in the mail id to access the original data. The data are encrypted and uploaded into the cloud server. Each data owner (e.g., patient) is a trusted authority of her own, who uses a ABE system to manage the secret keys and access rights of users in record. For the purpose of personal domain access (PSD), each PHR file is labeled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. Data owner needs to know the intrinsic data properties of PSD for encrypting the data. Based on the user permission record access is encouraged and sensitive attribute are hidden using ABE Technique.

The owners upload AES-encrypted PHR files to the server. Each owner's PHR file is encrypted using AES in ABE system. The ABE, under a certain fine grained and role-based access and under a selected set of data attributes allows access to users in the PSD. In Key policy Attribute Based Encryption (KP-ABE) the access structure is associated with the key and the attributes are associated with the cipher text which allows only the authorized users to decrypt the cipher text. Hence the Key policy Attribute Based Encryption is adopted for personal domain [16].This provides security for the sensitive information stored on the cloud. It also reduces most of the computational overhead to cloud servers. Only authorized users can decrypt the PHR files.

The system supports break-glass access under emergency scenarios. The medical staffs can have temporary access when an emergency happens to the patient [17]. At that time the medical staff requests and obtains the secret key from the emergency department(ED). The ED needs to authenticate the medical staff who requests for the key. This paper contains about the survey of Health record in the cloud server and proposed ABE algorithm for authentication. This idea facilitates to publish the survey report with new security policy.

3.3 ABE Algorithm

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party. This algorithm involves 4 modules including key generation.

Setup(I,U)->(PK,MK) - The setup algorithm takes security parameter I as inputs and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters public key PK and the master secret key MK.

Encrypt(PK,M, S)->CT - Encryption algorithm takes public parameters PK, a Message M and a set of attributes S as inputs and outputs a ciphertext CT associated with the attribute set.

KeyGen(MK,A)->SK - The key generation algorithm produces a private key SK by taking inputs master secret key MK and an access structure A. Here the output is associated with the attributes.

Decrypt(SK,CT)->M - The decryption algorithm accepts a private key SK which is associated with access structure A and ciphertext CT that is also associated with attribute set and provides a message M if S satisfies A.

Algorithm 1: Setup phase

Input: P ϵ G1 and Q ϵ G2, a set of attributes H

Output: Public Key PK(G1,G2, P, Q, P_δ, γ), f{H1……H_N},

Master private Key MK(P_α)

1. Choose at random : α and δ ϵ Z_r

2.P_δ ⟵ [δ]P

3.P_α ⟵ [α]P

4. γ ⟵ $e_{opt}(Q,P)^\alpha$

5. **for** i ⟵ 1 to #H **do**

6. Generate a point H_i ϵ G1

7. **end for**

8. PK ⟵ (G1,G2, P, Q, P_δ , γ), {H1……H_N}

9. MK ⟵ (P_α)

10. **return** PK,MK

Algorithm 2: Encryption phase

Input: A message M, PK, an access structure S given as a u x t

Matrix and I ⊂ {1, 2,…….,u} as I = {i : ρ(i) ϵ H}

Output: Ciphertext C_T = {S,C,C_d, (C_1;D_1),...., (C_u,D_u)}

1. Generate a random vector u = (s, $y_{2,\ldots..}$, y_t) ϵ Z_r.

2. Calculate the column vector λ = Su^t

3. Generate another random vector x = ($x_{1,\ldots..}$ x_u) ϵ Z_r.

4. C = M ⊕ H_1 (γ^s)

5. C_d = [s]Q

6. **for** i = 1 to u **do**

7. C_i ⟵ [λ_i] P_δ – [xi]$H_{\rho(i)}$

8. D_i ⟵ [x_i]Q

9. **end for**

10. C_T ⟵ {S,C,C_d, (C1,D1),….., (C_u,D_u)}

11. **return** C_T

Algorithm 3: Key generation phase

Input: MK and a set of user's attributes H

Output: A private key SK = {K, L,$K_{1,\ldots..}$,K_{vH}}

1. Choose at random τ ϵ F_r

2. K ⟵ P_α + [τ] P_δ

3. L ⟵ [τ]Q

4. **for** i = 1 to v_H **do**

5. K_i ⟵ [τ]H_i

6. **end for**

7. SK ⟵ {K, L,$K_{1,\ldots..}$,K_{vH}}

8. **return** SK

Algorithm 4: Decryption Phase

Input: C_T and its matrix S, SK and its set of attributes H

Output: Plaintext M (if the attributes in SK satisfy the ciphertext's policy)

1. $\hat{S}$ ⟵ Reduce the matrix S by removing the rows and columns unrelated with the attributes in H

2. Find the determinant Δ ⟵ Det(S) ϵ F_r

3. Calculate the vector ω as the first row of S^1

4.**for** i = 1 to v **do**

5. $C_i^{\omega i}$ ⟵ [ωi]C_i

6. $K_{\rho(i)}^{\omega i}$ ⟵ [ωi]$K_{\rho(i)}$

7. **end for**

8. M = C⊕H_1((e(Cd,C_iK) · e(L, $\sum_{i\epsilon H} C_i^{\omega i}$) · $\prod_{i\epsilon H}$ e(D_i, $K_{\rho(i)}^{\omega i}$))$^{1/\rho}$)

9. **return** M

4. RESULT AND DISCUSSION

Around 2500 KB of text documents were collected and performance analysis of ABE algorithm was carried out by decrypting the documents using different algorithms as tabulated in Table.1. The experiments were done using a system with Pentium-IV processor, 80GB RAM. Table 1 shows the time taken by different encryption algorithms for different size of data. The experiment results reveal that Advanced Encryption Standard (AES) is faster and best suited for large databases (Fig.3). The other algorithms can be ordered as DES, 3-DES, RC4, and finally the Blowfish algorithm.

Table 1: Time taken for Different Encryption Algorithm

File size(kb)	DES	RC4	AES	Blowfish	3DES
500	1.88	4	0.43	4	1.94
1000	5.99	5.1	0.7	5.2	5.8
1500	8.3	7.32	0.92	7.5	8
2000	9.8	9.9	1.4	9.9	9.57
2500	13.1	12.8	1.99	13.4	12.99

Table 2: Encryption time of documents using AES and ABE

Document size(KB)	Time taken by ABE (sec)	Time taken by AES (sec)
20	0.012	0.027
40	0.038	0.043
60	0.05	0.059
80	0.063	0.072
100	0.12	0.15

This implementation uses a 160-bit elliptic curve over a 512-bit finite field. The Fig. 4 shows the running time comparison of ABE and AES while encrypting the data mentioned in Table 2. The running time of ABE encryption is almost linear with respect to leaf nodes. But AES is not efficient for encrypting small amount of data. Hence a secure infrastructure for privacy preserving personal health record system is build using ABE.

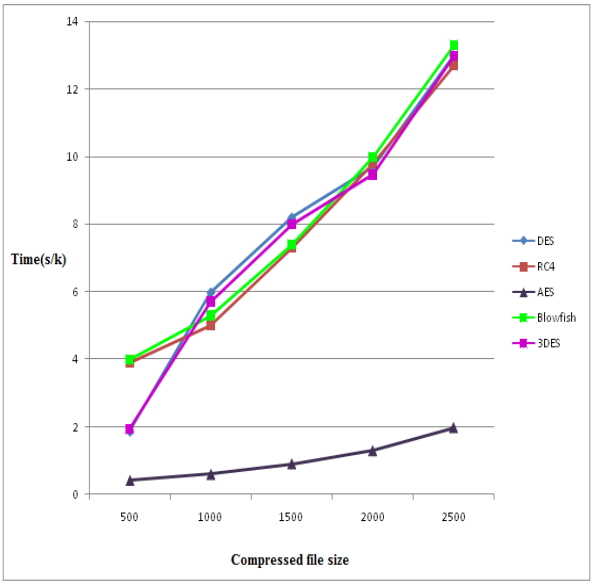

Fig.3 Performance Comparison of DES, RC4, AES, Blowfish, 3DES

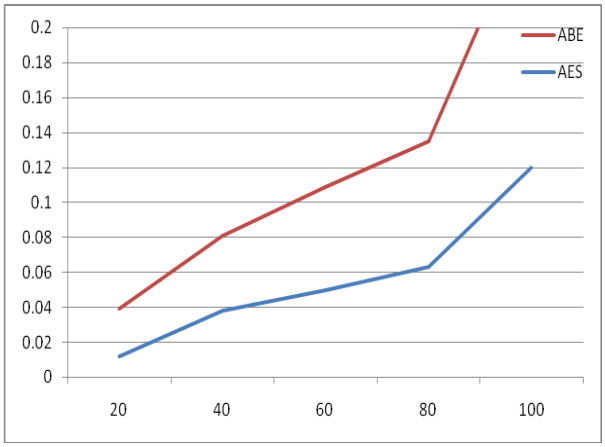

Fig. 4 Performance comparison of ABE and AES

In the figure the detailed computational timing results for all algorithms is shown. In this scheme, revocation of a user requires a minimum set of data attributes that makes the access structure weak. Our scheme has much smaller secret key size and the size of ciphertext generated is also smaller. Compared with existing revocable ABE schemes, the main advantage of scheme is small rekeying message sizes. To revoke a user, the maximum rekeying message

size is linear with the number of attributes in that user's secret key. These indicate our scheme is more scalable than existing works.

Hence, the ABE scheme is quite faster and more suitable for the time costs of key generation, encryption, and decryption processes are all linear with the set of attributes. From the system aspect, each data owner uses the ABE scheme for setup, key generation, Encryption and Revocation and each PSD and PUD user decrypts the file in less time. The Attribute Authority (AA) is used for setup, Key Generation, User Revocation. In case of 50 attributes, they all take less than 0.5s.Hence from the results, ABE is more scalable and efficient to implement in Personal Health Domain as it reduces the complexity of key management.

5. CONCLUSION

Though it is proved that hashing based authentication algorithms can provide security as the key generated by them cannot be rehashed, our experiments proved that ABE is more secure. Researchers have found weakness in SHA1 and are subjected to collision attack which is theoretically broken. Hence it is considered no longer secure. But ABE is not rendered to collision attack because the keys are generated from different set of attributes. As we employed ABE for data encryption and authentication, a testing can be performed on the security of the data in the future work. This work can be extended to encrypt multimedia data and to nested authentication in distributed environment.

CONFLICT OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Gurpreet Singh, Supriya. April 2013, "A Study of Encryption Algorithms for Information Security", *International Journal of Computer Application*, Vol.67, No.19,33-38.

[2] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou and Robert H. Deng. February 2014, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", *IEEE Transactions on Parallel and Distributed Systems*, Vol.25, No. 2.

[3] Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh. 2013, "A Survey of Cryptographic Algorithms for Cloud Computing", *International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*, 141-146.

[4] Pooja R. Vyawhare, Prof.Namrata D. Ghuse. 2015, "User Anonymous Authentication Scheme for Decentralized Access Control in Clouds", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol.6, No.3, 2441-2447.

[5] Sumita Lamba, Ajaykumar. February 2014, "An approach for ensuring security in cloud environment", *International Journal of Advances in Computer Science and Technology (IJACST)*, Vol.3, No.2, 92-95. .

[6] Dhaval Patel, M.B.Chaudhari. June 2014, "Data Security In Cloud Computing Using Digital Signature", *International Journal for Technological Research in Engineering*, Vol.1, Issue 10, 1177-1180.

[7] Y.B.Gurav, ManjiriDeshmukh, "Scalable and Secure Sharing of Personal Health records in Cloud Computing using Attribute Based Encryption", International Journal of Science and Research (IJSR), Vol. 3 Issue 7, ISSN:2319-7064, July 2014.

[8] Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou. 2010, "Attribute based data sharing with attribute revocation", *ASIACCS,10*.

[9] Y.Pavani, Rajasekar, D.Krishna. 2014, "Cloud Storage with data sharing and security for Multi access network by Using AES", *IJESC*, 536-539.

[10] B.SriVarsha, P.S.Suryateja. 2014, "Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5(6), 7745-7747.

[11] Mehmet Hakan SATMAN. 2013, "Machine CodedGenetic Algorithms For Real Parameter Optimization Problems", Gazi University Journal of scienceVol.26, 85-95.

[12] Randeep Kaur, Supriya Kinger. March 2014, "Analysis of Security Algorithms in cloud computing", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Vol. 3 Issue 3.

[13] S.I.Shaik Hussain, V.Yuvaraj. March 2015, "Efficient and Secure Data Transactions using AES in P2p Storage Cloud", *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* Vol. 3 Issue 3.

[14] Vikas Vitthal Lonare, Prof.J.N.Nandimath. 2015, "Ensuring Distributed Accountability for Data Sharing in Cloud Using AES and SHA", *International Journal of Computer Science and Information Technologies (IJCSIT),*Vol. 6(1), 652-657.

[15] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem. December 2013, "Efficiency of Modern Encryption Algorithms in Cloud Computing", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),*Vol. 2,Issue 6, 270-274.

[16] Ajay Ambedkar .R, K. John Paul. 2013, "Achieving Security, Scalability and Efficiency Sharing of Personal Health Records in Cloud Computing", *International Engineering and Technology Research Journal (IETRJ),* Vol. 1(3), 104-111.

[17] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou. 2012, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", *IEEE Transactions on Parallel and Distributed Systems*.