JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 823-836 (2017)
DOI: 10.6688/JISE.2017.33.3.14

Improved Searchable Attribute Based Encryption in Cloud

SANGEETHA D.[1] AND VAIDEHI V.[2]
[1]*Madras Institute of Technology*
Anna University
Chennai, 600044 India
[2]*Vellore Institute of Technology*
Chennai, 600127 India
E-mail: dsangeetha@mitindia.edu; vaidehiaucmit@gmail.com

The development of online electronic personal data leads to the trend that data owners prefer to remotely outsource their health information to the cloud. Personal Health Record (PHR) is a developing online service model that allows PHR users to enjoy high quality retrieval of health record and storage space. However, an efficient secured share and search for the outsourced health data is a difficult task. Searchable Attribute Based Encryption (SABE) enables the data owners to efficiently share his/her data to a specified group of users. It requires the health data to preserve its searchable property while it is shared among public domain users like doctors and researchers. Moreover, it facilitates keyword search on ciphertext which consumes a considerable amount of search time in keyword query processing. To minimize the search time to retrieve the related health attributes from PHR database, this paper proposes an Improved SABE (ISABE) for PHR in the cloud. Nowadays, Global Positioning Service (GPS) is combined with mobile technology and it became part and parcel of our lives. However, most of the existing cryptographic schemes are location independent. Therefore, Location Based Encryption (LBE) allows a secure communication of mobile nodes by restricting unauthorized access of sensitive information at a specific location and time. But the existing GPS technology has several inconsistencies like the triangular problem and number of keys generated for the particular user within the region of interest. To minimize the number of keys generated for the mobile users in an environment with location based services, this paper proposes an Enhanced Location Based Encryption (ELBE) with threshold limit to enforce non-repudiation. From the experimental results, it is found that the proposed ISABE with ELBE improves the efficiency of the PHR system in the cloud by minimizing the storage complexity, keyword query search time and Key management for PHR users in a multi owner cloud environment.

Keywords: personal health record, cloud computing, attribute based encryption, searchable attribute based encryption, location based encryption.

1. INTRODUCTION

In recent years, information systems have turned out to be progressively essential in healthcare delivery. Personal Health Record (PHR) is an online health model for sharing health information among patients, doctors, researchers, *etc.* PHR created by a PHR owner (patient) is stored on a cloud server which uses the analytical service of the cloud service providers [3]. Generally, the PHR system allows a user to create and track his/her personal data pervasively through the web which has made the storage, retrieval, and

Received July 22, 2016; accepted September 21, 2016.
Communicated by Balamurugan Balusamy.

sharing of the medical information more efficient. Each PHR user possesses control over their own health data and they can effectively share their records with a wide range of PHR users, including doctors, friends, researchers and insurance agents in a cloud environment.

The cost of building and maintaining of data centers causes the PHR services to be provided by semi trusted third party cloud service providers. The main security issue with PHR is whether the patients could actually accomplish control on sharing their sensitive Personal Health Record (PHR). The patients fail to establish control over their PHRs when stored in cloud servers and the service providers cannot provide strong privacy assurance.

Since cloud computing is an open platform, the semi-trusted servers are subjective to severe security attacks [11]. Issues such as privacy exposure, unauthorized access to health records *etc.* are the important challenges in achieving fine-grained, cryptographically designed access control mechanism.

The existing encryption schemes such as symmetric or public key cryptography fail to provide a scalable access control. A suitable approach to address this issue is Attribute-Based Encryption (ABE), first proposed by Sahai and Waters [2]. ABE schemes can be divided into two categories: Ciphertext Policy ABE (CPABE) and Key Policy ABE (KPABE) [2], depending on the access policy is embedded into the ciphertext or the user's private key. Both CPABE and KPABE is proved to be efficient in preventing unauthorized PHR users from accessing the sensitive health information stored in semi-trusted servers. Such properties of ABE schemes are very attractive in the area of the cloud storage domain. Though traditional ABE guarantees the confidentiality of the data [2], it offers the limitation in data searching.

To facilitate data searching in the ciphertext, the concept of Searchable Encryption (SE) [6] was introduced. It is a cryptographic technique that ensures the security of outsourced data by encryption while supporting keyword search on the ciphertexts. Searchable Attribute Based Mechanism [9] enables searching on the encrypted ciphertext and also the corresponding search keyword(s) can be updated even after the data is shared. But the secret key holder needs an interaction with the key Generator when generating a keyword query trapdoor [7].

Location based encryption (LBE) [5], enhances security by integrating the position and time into encryption and decryption mechanisms. After determining the target coordinates, it is attached with the secret key to generate ciphertext. Decryption can be performed on the cipher text only when the coordinates received from the GPS receiver match with the target coordinates. The existing Location based encryption scheme renders another layer of security to the traditional encryption methods, thereby restricting the decryption process to a particular location. Moreover, the existing GPS Technology has several issues like Triangular problem and the number of keys generated for the particular user within the region of interest [5].

Therefore, the existing issues in SABE like a keyword search trapdoor which affects the retrieval time of health records when ported onto cloud should be addressed. In this work, an improved searchable attribute based encryption (ISABE) for PHR in the cloud is proposed. It enables searching on encrypted health records in the cloud using inverted index data structure with minimal storage and retrieval time complexity. Moreover, this paper focuses on Location based encryption with Enhanced LBE (ELBE) to

enforce trustworthiness in PHR cloud thereby reducing the number of keys generated in a particular area of the PHR user.

The paper organization is as follows. In section 2, the related work is introduced. In section 3, proposed improved searchable attribute based encryption (ISABE) and Enhanced Location Based Encryption (ELBE) algorithms are presented. Security and performance analysis of the proposed work are discussed in section 4. Finally, the conclusion of the paper is presented in section 5.

2. RELATED WORK

This section provides details about the various attribute based encryption techniques for secure sharing of PHR in a cloud environment. The advantages of Searchable attribute based encryption and Location based encryption schemes are discussed.

2.1 Personal Health Record (PHR)

Homomorphic encryption of data was proposed to maintain trustworthiness of the outsourced PHR. This ensures the PHR users control over their own private health information with data auditing to verify the correctness of PHRs stored in third party cloud servers [3]. Homomorphic encryption technique also supports modification of access policies or file attributes dynamically, efficient on-demand user/attribute revocation and break glass access under emergency scenarios while protecting the original data. For secure data outsourcing and key management, the PHR setup is divided into multiple security domains. Fine grained access control ensures efficient data sharing and confidentiality. It assign set of rights to a specific PHR user supporting Broadcast encryption, Attribute Based Encryption, Attribute-set Based Encryption, Hierarchical Based Encryption, Hierarchical attribute-set based encryption, Key-policy attribute based encryption, ciphertext-policy attribute based encryption, ciphertext-policy attribute-set based encryption, and patient controlled encryption techniques. Attribute Based Encryption technique overcomes the challenges of fine grained access such as scalability, flexibility and uses Multi-Authority ABE that ensures patient privacy [11].

2.2 Attribute Based Encryption (ABE)

Attribute Based Encryption for encrypted access control of encrypted data overcomes the selective share only at the coarse-grained level. A new cryptosystem called the Key-Policy Attribute-Based Encryption (KPABE) was developed [2] where ciphertexts are labeled with sets of attributes and private keys are associated with access structures. The user is able to decrypt only if his access structure matches the attribute set of the ciphertext. Ciphertext Policy Attribute Based Proxy Re-encryption (CPABPRE) [8] overcomes the Chosen CiphertextAttack (CCA) for the first time and supports Attribute Based Proxy Re-encryption with monotonic access structures.This technique extends the traditional proxy reencryption by permitting the transformation of a ciphertext with an access policy to same plain text with a different access policy provided the proxy server gains no knowledge about the plaintext. A DFA-Based Functional Proxy Re-Encryption

Scheme [8] encrypts a message into a ciphertext of arbitrary length string. The user can decrypt the message if and only if the DFA associated with his secret key accepts the string. The above encryption can be transformed to another ciphertext associated with a new string by a semi-trusted proxy that has the re-encryption key but cannot access the underlying plaintext. This scheme provides flexibility of users to assign their decryption rights to others but does not support conversion to a prime order bilinear group.

2.3 Searchable Attribute Based Encryption (SABE)

Searchable Encryption (SE) [1] scheme allows users to search keyword on encrypted data while protecting the sensitive information. To share data among multiple users with different access rights, searchable encryption with fine grained access control under multi-user setting was proposed [8]. To achieve a user collusion resistant property, SE [4] and Ciphertext-Policy Attribute Based Encryption (CP-ABE) techniques are combined which provides less computation cost, overcomes the problem of key sharing, provide security with dynamic and efficient user revocation. Existing technique supports either searchable encryption or Attribute Based Encryption. Searchable Attribute based Encryption with proxy re-encryption [9] allows PHR users to efficiently share their data to a specific group of people thereby maintaining its searchable property. This technique has proven to be secure against ciphertext attack, but has the challenges of keyword search time and storage space complexity.

2.4 Location Based Encryption (LBE)

Cloud computing has serious security challenges like data access control over critical and confidential information. To overcome the existing security challenges, Abolghasemi introduced Location Based Encryption which adds a new security level to the existing security measures that can be used in several places [10]. Location Based Encryption is a technique to secure data using encryption algorithm and the user's position. The encryption key is generated by encoding estimated receiver's location information with a random key for the data. The receiver can decrypt the ciphertext only at the target location. Location based encryption technique is innovative and provides an additional layer of security, ensuring confidentiality, authentication and simplicity by restricting decryption only at specific locations [5]. The idea of Geo-encryption with Position, Velocity and Time (PVT)-to-Geolock mapping function is used as a key mechanism to ensure that the data can be decrypted successfully but faces a challenge of key management.

3. PROPOSED IMPROVED SABE (ISABE)

An Improved Searchable Attribute Based Encryption in cloud introduces an Inverted Index based Searchable Attribute Based Encryption. It guarantees the keyword search ability of the cipher text to be maintained even after the sharing of the cipher text and it reduces the storage complexity. This model makes use of the PHR cloud where the PHR users like doctors, patients, *etc.* can upload their health records and can assign the access control list for the set of documents. The encrypted documents will be stored in a PHR

database and each attribute authority will be delegated with the set of attributes.

The proposed architecture of ISABE is shown in the Fig. 1. The public domain PHR users like researchers are allowed to enter into the system either through the PHR web portal or using PHR mobile applications. Once the researchers login into their system using their Global Identifier GID, it has been replaced by the token which ensures the preservation of user's privacy. Then the researchers can view the list of their attributes they are accessible to (*i.e.* their access control list). The researchers are then provided with their public and private key from the Certificate Authority.

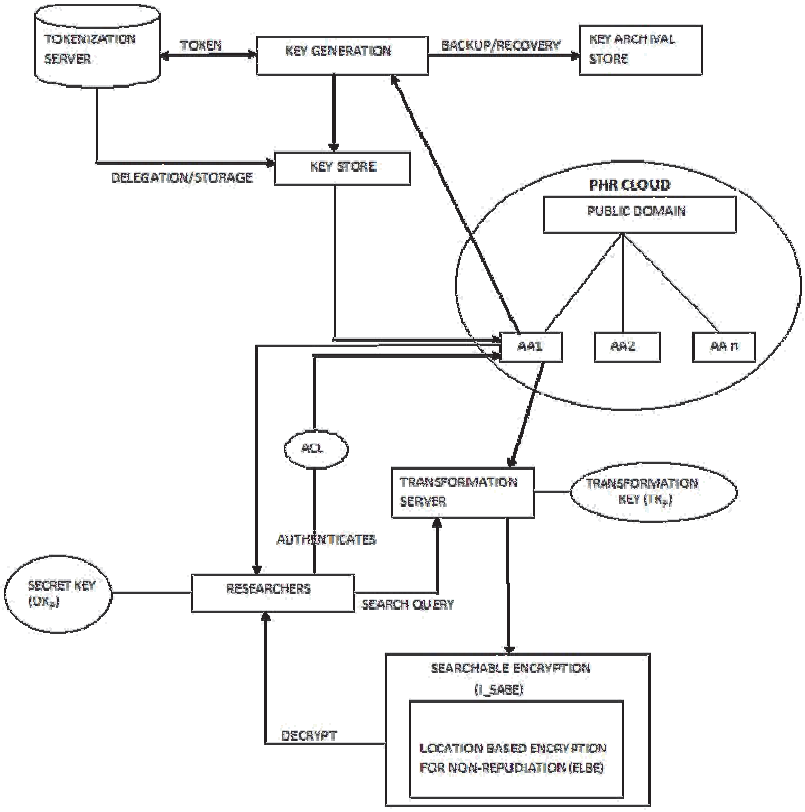

Fig. 1. Improved searchable attribute based encryption (ISABE).

The private key of the user is split into a "transformation key" (TK) and a secret key (DK). The transformation key is shared publicly with a proxy server named as Transformation Server (TS), while the secret key DK is kept private by the user. A ciphertext CT generated using ABE is stored in the Cloud Storage Server (CSS). CT is submitted to the TS which uses the key TK to transform CT into CT' associated with keywords. From CT' the user is able to recover the message associated with the queried keyword using the secret key DK. Thus, the user's transformation key can transform any ABE ciphertext satisfied by user's attributes, without exposing any information of the underlying message thereby saving the local computation time significantly. The researcher can in-

put a Keyword Query like 'age > 50'. On input the keyword, the transformation server indexes the users associated ABE cipher text and then searches the keyword in the encrypted cipher text. Then the resultant documents are encrypted using location based encryption and it is sent to the receiver side. The receiver using their location information and the secret key provided to them can decrypt the set of all ciphertext associated with the keyword query.

3.1 Inverted Index Based Searchable Attribute Based Encryption (II-SABE)

The IISABE module allows the PHR users like researchers to make a search on the encrypted documents with minimal storage complexity. The architecture of the II-SABE module is described in the Fig. 2. The private key of the user is split into the transformation key and the secret key. The transformation server makes use of the transformation key to access all the cipher text associated with the Access Control List of the user from the encrypted database. Once the encrypted documents are retrieved the transformation server, it makes use of the Inverted Index Data Structure and does a keyword search in the encrypted ciphertext. The resulting ciphertext associated with the keyword query is then re-encrypted and sent to the receiver side for decryption. The notations used in ISABE are shown in Table 1.

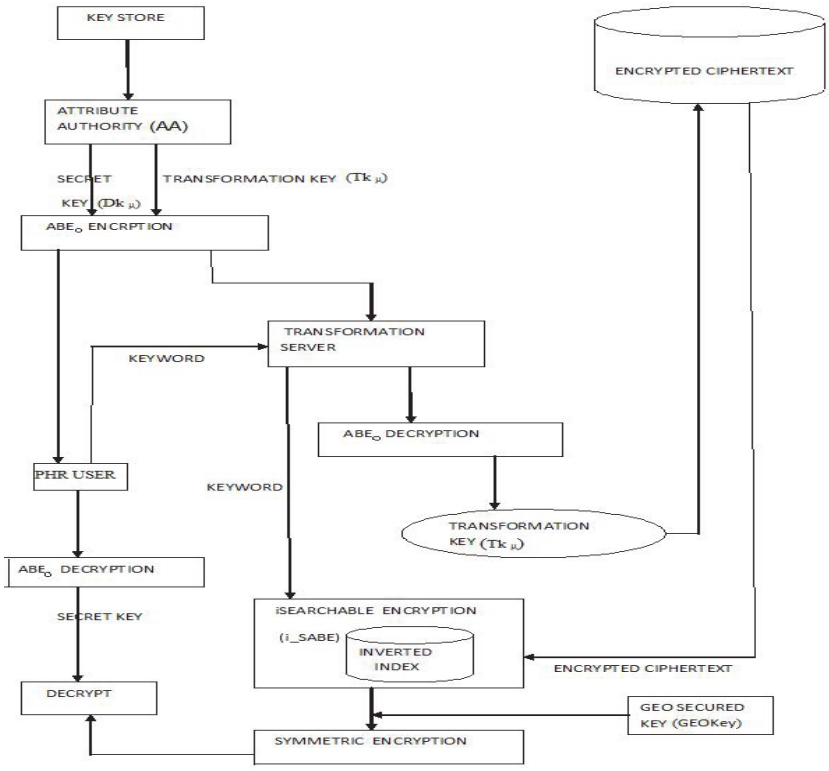

Fig. 2. Inverted index based searchable attribute based encryption.

ISABE Algorithm

- Setup (1^{λ}, U) $\rightarrow$ (mpk, msk)
  On input a security parameter λ and a universe of description U, output a master public key (mpk) and a master secret key (msk).
- Key Gen (msk, μ) $\rightarrow$ (Tk_{μ}, Dk_{μ})
  On input msk and a description $\mu \in \{0, 1\}^*$, output a transformation key (Tk_{μ}) and a secret key (Dk_{μ}).
- Extract Doc (Tk_{μ}, DB) $\rightarrow$ CT
  On input transformation key and an encrypted database (DB), output a set of ciphertext associated with the description μ (CT).
- I_search (KW, CT) $\rightarrow$ CT′
  On input a keyword (KW) and CT, output a set of ciphertext (CT′) associated with the particular keyword (KW).

Sender

- Enc (Tk_{μ}, $GKey_{sender}$, CT′) $\rightarrow$ CT1′
  On input a transformation key, geo secured key and CT′, output a location based encrypted document CT1′.

Receiver

- Dec (Dk_{μ}, $GKey_{receiver}$, CT1′) $\rightarrow$ PT
  On input a secret key, Geo Secured Key and CT1′, output a plain text satisfying the keyword KW.

Table 1. Notations in ISABE.

SL:NO	Symbols	Description
1	ƛ	Security Parameter
2	mpk	Master Public Key
3	msk	Master Secret Key
4	M	Access Structure of the user
5	Tk_{μ}	Transformation Key
6	Dk_{μ}	Secret Key
7	DB	Encrypted Database
8	CT	Cipher Text
9	KW	Keyword
10	CT′	Cipher text associated with KW
11	CT1′	Cipher text associated with μ
12	$GKey_{sender}$	Geo Secured Key for sender
13	$GKey_{receiver}$	Geo Secured Key for receiver
14	PT	Plain Text

Enhanced Location Based Encryption (ELBE)

To enforce Non Repudiation, the proposed ISABE uses Enhanced Location Based Encryption. The receiver location is constantly updated on the transformation server. The

transformation server estimates the receiver location based on the recorded location information. Then, using this information, a geo tag is generated which is associated with the transformation key to generate geo secured key. Using the geo secured key with the symmetric encryption algorithm, the cipher text which is associated with the keyword query is reencrypted and sent to the receiver side for decryption.

At the receiver side, the user computes the geo tag using their location information. And with the geo tag and the secret key associated with them, the user generates the geo secured key. Using the geo secured key and the symmetric algorithm the researcher can decrypt the cipher text associated with the keyword. While computing the geo tag using the user latitude, longitude, time, velocity; the proposed framework introduces an additional dimension parameter called Tolerance distance (*i.e.* Threshold Limit). The proposed module ELBE architecture is shown in Fig. 3. With the use of this dimension parameter the number of keys generated for the particular region of PHR users is minimized. The notations used in ELBE is shown in Table 2.

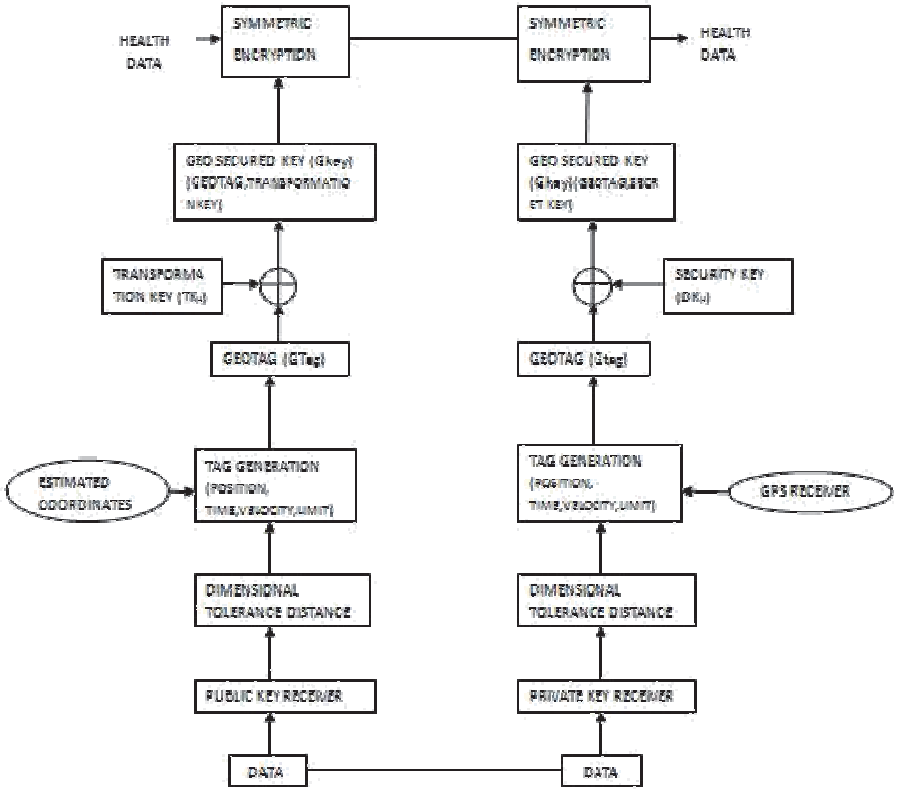

Fig. 3. Enhanced location based encryption.

ELBE Algorithm

- $x \leftarrow$ (latitude (xor) longitude)
- $y \leftarrow$ (Time (xor) Velocity)
- $z \leftarrow (x \text{ (xor) } y)$

- Tag Generation (z, limit) → GTag
  On input the coordinates, time, velocity and the threshold limit, output a Geotag.

Sender

- Key Gen (GTag, Tk_{μ}) → $GKey_{sender}$
  On input a GeoTag and the transformation Key, output a Geo Secured Key.

Receiver

- Key Gen (GTag, Dk_{μ}) → $GKey_{receiver}$
  On input a GeoTag and the Secret Key, output a Geo Secured Key.

Table 2. Notations in ELBE.

SL:NO	Symbol	Description
1	GTag	Geo Tag
2	$GKey_{sender}$	Geo secured key for sender
3	$GKey_{receiver}$	Geo secured key for receiver
4	TK_{μ}	Transformation key
5	DK_{μ}	Secret Key

4. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Security Analysis

The proposed ELBE is secure against cryptographic attacks like replay attack between users (theorem 1) and wormhole attack between the users at different location (theorem 2) and is proved as follows:

Theorem 1: The proposed ELBE scheme is resistant to replay attack.

Proof: Assume Enhanced Location Based Encryption algorithm broadcasts message '*m*' with token '*tk*' at location '*l*'. An attacker at the same time listens to the medium and records '*m*' at time '*t*'. A legitimate user may listen to the broadcast medium. The attacker will not have the knowledge of items like secret key, tokens *etc*., other than the original location and the time '*t*'. The session token '*tk*' will be valid during a time, a time period '*d*'.

At time $t+d$ the algorithm chooses a new session token and henceforth the message '*m*' becomes invalid. At time $t+d+\delta$ where $\delta>0$ the attacker will broadcast the message. The legitimate user listens to *m*. Both Enhanced Location-Authentication algorithm and attacker will listen to the reply.

Without the knowledge of the secret keys the attacker cannot decrypt the reply message. The receiver will run the decryption algorithm at time $t+d+\delta$. At that time the token will become invalid and thus authentication will fail.

Theorem 2: The proposed ELBE scheme is resistant to wormhole attack.

Proof: Assume the attacker does the replay attack, and has knowledge of the original location '*l*'. He also has a direct network connection through a secondary channel to another location '*p*'. The token generated by Enhanced Location-Authentication algorithm within the time *t+d* at location '*l*' is different from the token generated at location '*P*'. Thus authentication will fail.

Performance Analysis

Implementation Details

This section describes the implementation details used for the design of proposed ISABE. An OpenNebula private cloud environment is installed and the instances are created. The application is deployed on Lampp server, using an instance of Open Nebula private Cloud. A Mysql server is deployed on the virtual instance and a PHR database is created. A sample PHR dataset which contains the patient information like their heart rate, breath rate, blood pressure, *etc.*, along with the sensitivity level of the patient is taken for implementation.

When a PHR user request access to the system, his/her credentials is validated based on the information stored in the user table of the PHR Database. The user can request a health record of a patient using a search query. The request is granted and the details retrieved and decrypted from the PHR database only if the user's private key attributes satisfy the access structure. Similarly, when the user requests to upload a health record, it will be encrypted and then uploaded to PHR database.

False Measurements

The false measurements of the proposed ELBE are given based on False Negative and False Positive. The position of the user is shown in Table 3. False Negative is a case where the estimated parameter of the user is outside the security range,even if the real position of the user is inside. False Positive is a case where the estimated parameter of the user is inside the security range, although the real position of the user is outside.The false measurements of the proposed ELBE are shown in Fig. 4.

Table 3. Position of the user.

	User	Attacker
The test is positive	True Positive (TP)	False Positive (FP)
The test is negative	False Negative (FN)	True Negative (TN)

False Positive = FP/(FP+TN)
False Negative= FN/(FN+TP)

Parameters Considered

To measure the performance of the Improved searchable attribute based encryption for personal health record in the cloud, the parameters considered are the search time and the number of keys generated for users like doctors, researchers and relatives. The number of keys generated in the proposed ELBE and the existing LBE in the public domain

based on the number of users is shown in Fig. 5. The search time of the existing SABE and the proposed ISABE for the public domain users is shown in the Fig. 6.

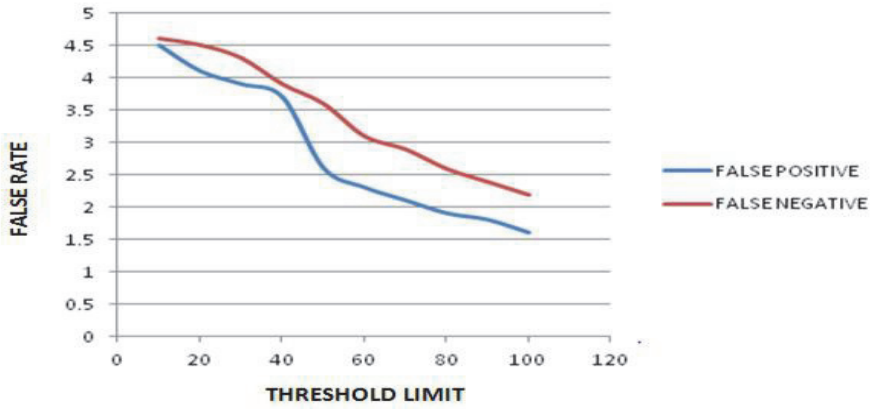

Fig. 4. False measurements of proposed ELBE.

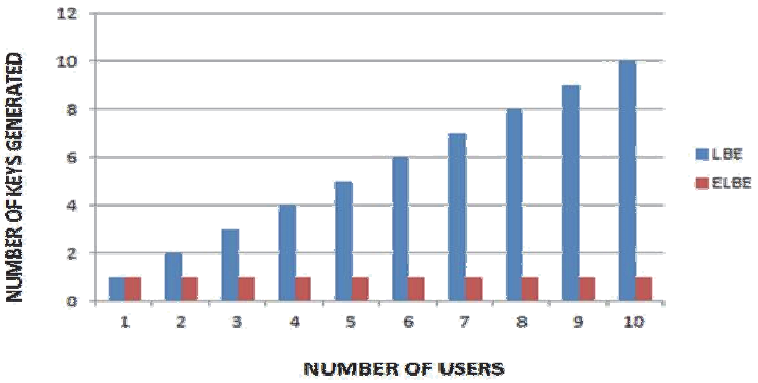

Fig. 5. Performance measure of ELBE.

The proposed ISABE maintains a User database which contains Global Identity (GID) of the registered users by which they can perform successive access of PHR in Open Nebula cloud. A policy database which maintains the roles representing the relationship that exists between the user and the PHR owner is used for allocating the user to their respective Attribute Authorities for obtaining the secret keys. After proper authentication, the user obtains the PHR access in the cloud based on the role id.

The performance measure of the ELBE model is evaluated and compared with the existing LBE. In the existing LBE system the keys generated increases linearly as the number of users within a region are increasing. The ELBE model generates a constant no of keys for all the users within the region of interest. Thus the key management complexity is much reduced in Enhanced Location based Encryption system.

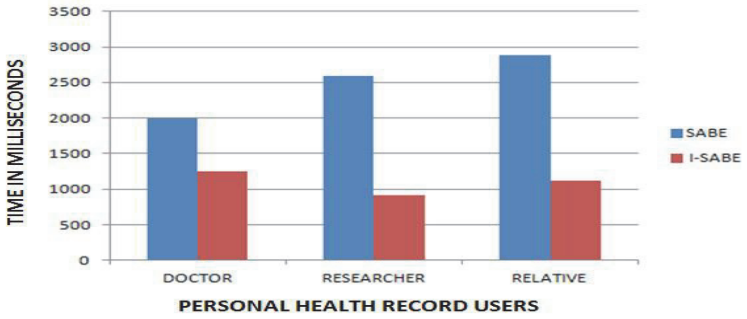

Fig. 6. Performance measure of ISABE.

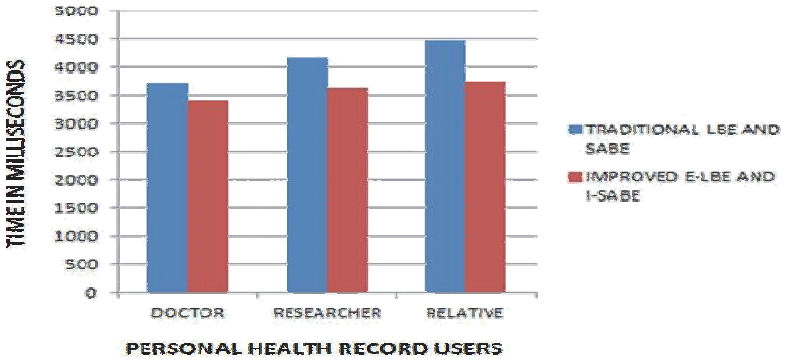

Fig. 7. Performance measure of ISABE and ELBE.

The performance measure of the ISABE system is evaluated and compared with the existing SABE system. In the existing system when the user wants to search on the encrypted ciphertext, he wants to download the ciphertext from the data store, decrypt and then search on the encrypted ciphertext. In the inverted index based searchable attribute based encryption, the users are allowed to search on the encrypted ciphertext and then decrypt and download only the text related to the search query. Thus the search time is reduced when compared to the existing SABE system as shown in Fig. 7.

The overall performance measure of the proposed ISABE and the enhanced location based encryption system is evaluated and compared with the traditional SABE and LBE system. The improved system uses inverted index data structure with interval limits in searchable attribute based encryption. It further introduced the additional dimension tolerance limit in location based encryption to reduce the key management complexity. Thus the overall running time of the system is considerably reduced in the new improved system.

The time complexity is computed for the proposed scheme, namely ISABE and ELBE and it is shown in Table 4. To compute the time complexity, the parameters such as N which represents the number of attribute authorities, I which represent the Attributes in the system I_c and I_j represents the Index set of Attribute Authorities, n which represents the number of PHR users in a particular area and finally A_c representing the attribute set of authorities is considered.

Table 4. Time complexity of existing and proposed schemes.

Operation	Existing Scheme	Proposed Scheme	
		I_SABE	ELBE
Setup	$O(1)$	$O(1)$	$O(1)$
AA-Setup	$O(2N+M)$	$O(N)$	$O(N)$
Encryption	$O(I+1)$	$O(I_c)$	$O(I_c)$
Decryption	$O(2I)$	$O(I*I_j)$	$O(I_c*A_c)+I_c$
KeyGeneration	$O(n)$	$O(1)$	$O(1)$

The above table ensures that the key management complexity in the proposed technique is constant when compared with the existing scheme. The complexity of encryption remains same as the existing technique. The decryption time complexity when compared with the existing scheme is much reduced in the proposed improved searchable attribute based encryption.

5. CONCLUSION

An Improved Searchable Attribute Based Encryption for Personal Health Record in cloud guarantees that the keyword search ability of the ciphertext can be remained after the sharing of the ciphertext. It reduces the storage complexity and keyword retrieval time complexity using the Inverted Index based SABE. It provides an additional layer of security using LBE with a dimension threshold limit to overcome the inconsistencies by GPS servers and reduces key Management complexity. The secret key of the user is used to overcome false acceptance rate and false rejection rate. From the experimental analysis, it is found that the proposed Improved SBE is efficient for sharing of PHR in a multi owner cloud environment.

REFERENCES

1. A. Petcher and G. Morrisett, "A mechanized proof of security for searchable symmetric encryption," in *Proceedings of IEEE 28th Computer Security Foundations Symposium*, 2015, pp. 481-494.
2. A. Sahai, V. Goyal, O. Pandey, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *IEEE Transactions on Parallel and Distributed Systems*, 2005, pp. 89-98.
3. B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, Vol. 10, 2015, pp. 1384-1393.
4. B. Wang, W. Son, W. Lo, and Y. T. Hou, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in *Proceedings of IEEE Conference on Computer Communications*, 2015, pp. 2092-2100.
5. B. Manoj V, B. Harshad D, P. Dhiraj M, B. Pratik B, "Location based encryption-decryption approach for data security," *International Journal of Computer Applica-*

tions Technology and Research, Vol. 3, 2014, pp. 610-611.
6. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," *International Journal of Computer Applications*, 2000, pp. 44-55.
7. J. Yang, C. Fu, N. Shen, Z. Liu, C. Jia, and J. Li," General multi-key searchable encryption," in *Proceedings of the 29th International Conference on Advanced Information Networking and Applications Workshops*, 2015, pp. 89-95.
8. K. Liang *et al.*, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics and Security*, Vol. 9, 2014, pp. 1667-1680.
9. K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, Vol. 10, 2015, pp. 1981-1992.
10. M. S. Abolghasemi, M. M. Sefidab, and R. E. Atani, "Using location based encryption to improve the security of data access in cloud computing," in *Proceedings of International Conference on Advances in Computing*, *Communications and Informatics*, 2013, pp. 261-265.
11. Y. Zheng, K. Ren, M. Li, S. Yu, 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, 2013, pp. 131-143.

Sangeetha D. received the BE degree from the University of Madras, India in 2001 and ME degree from Anna University, India in 2008, both in Computer Science. She is currently an Assistant Professor in the Department of Information Technology, Anna University, India. She is pursuing her Ph.D. in Information and Communication Engineering at Anna University, India. Her research interests include cryptography and network security, cloud computing and Service oriented architecture. Her current focus is on secure data services in cloud and computation.

Vaidehi V. received the BE and ME degrees from Anna University, India. She received her Ph.D. degree in Information and Communication Engineering at Anna University, India in 1997. She is currently Dean and Senior Professor in the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai. She is a retired Professor from Anna University, India. Her research interests include wireless sensor networks, security, parallel computing, cloud computing and networks. She is serving as the reviewer for NCC (National Conference on Communications) organized by IIT and IISC from 2008 onwards. She has won Active Consultant/Research Award by CTDT, Anna University, 2011 and Faculty Award by Microsoft in 2011. She received ACU (Association of Commonwealth Universities) Fellowship to visit Universities in Singapore and Malaysia for a period of 3 months during April-June 1995.