Preserving Privacy in Cloud Assisted Mobile Access

Gayathri K, Lavanya S, Maria Justina Z, Virajitha S
Department of Computer Science and Engineering
T John Institute of Technology
Bengaluru, India

Roopashree S
Department of Computer Science and Engineering
T John Institute of Technology
Bengaluru, India

***Abstract*—The timely treatment of medical emergencies in e-healthcare system enables better healthcare service provisioning, improved quality of life and helps saving life. The Proposed system is built on privacy issues with the help of cloud service models. Some of the remarkable features that the propound system renders are efficient key management, Privacy preserving data storage and retrieval at emergencies and auditability for misusing health data. It also incorporates a secure indexing method for privacy preserving keyword search which is based on redundancy and hides both search and access patterns and also consolidates the concept of attribute based encryption.**

***Keywords*— Access control, auditability, e-health, privacy, cyberspace.**

I. INTRODUCTION

Electronic healthcare system provides services that are supported by mobile devices such as homecare and remote monitoring, allows the patient to retain minimum intrusion in their daily activities. Remarkably it allows patient only with higher need to be admitted and this reduces the hospital possession. The e-healthcare systems are popular and they cover the digital process in health while people lose their privacy over their personal information once they enter the cyberspace, is the notional environment in which communication takes place over the computer networks and due to this it disclosed 8 million patients health information within two years. This made the protecting privacy in the cyberspace more challenging.

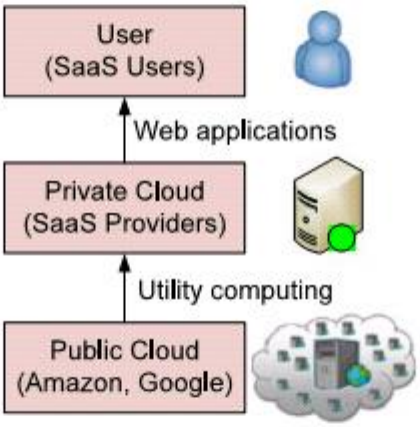

Fig. 1. SAAS Service Model

A software as a SaaS provider provides cloud service by using the infrastructure of the public cloud provider as shown in Fig.1. Cloud assisted mobile health networking is inspired by flexibility, cost efficiency and power. The total claim capture and control management for insurance company using amazons elastic compute cloud to process the millions of claims daily.

II. PRELIMINARIES

A. *Searchable Symmetric Encryption (SSE)*

SSE was first proposed by Goh[1], and later improved by Curtmola et al.[2]. SSE enables the data owners to store encrypted documents on remote server. This is modeled as genuine-but-curious party, and it also provides a way to search over the encrypted documents. The most important is that there is no information leakage to any party except the data owner. Thus there is a guarantee of privacy.SSE consists of following algorithms.

KeyGen(s): The function is used by the users to generate keys to initialize scheme. It takes security parameter *s* and outputs a secret key *K*.

BuildIdx(D, K): User executes this function to build the indexes, denoted by *I*, for a collection of document *D*. It takes the secret key *K* and *D* and outputs *I*.

*Trapdoo*r(*K, w*): User runs this function to compute a trapdoor for a keyword w, allows searching for this keyword. A trapdoor *Tw* should leak the information about *w* as little as possible. It takes secret key *K* and the keyword *w* and outputs the respective trapdoor T_W.

Search(I, T_W*):* This function is executed by the remote server to search for documents containing the user defined keyword *w*. The function takes the build secure index *I* and the trapdoor *Tw*, and outputs the identifier of files which contains the keyword *w*.

Document is represented by an identifier and corresponds to a node. All documents in *D* are encrypted and stored in remote servers. The index I is made of two data structures, that is an array *A*, for storing the nodes and a look-up table *T*, for keeping information that’s allows the remote server to locate the elements in *A*. All nodes are encrypted with random generated keys and stored as entries in *A* in a random order. T_W consists of an output of a random number generator, for locating entries in *T*, and an output of a pseudorandom permutation function, for encrypting entries, given the input *w* of pseudorandom algorithms.

B. Threshold Secret Sharing

Secret sharing is a mechanism for sharing secret information among multiple entities so that the cryptographic power is distributed which at the same time avoid single point of failure. The goal is to divide secret S into n pieces of data *S1… Sn* in such a way that:

- Knowledge of any *k* or more *Si* pieces makes *S* easily computable.
- Knowledge of any *k-1* or fewer *Si* pieces leaves *S* completely undetermined. This scheme is called (*k*, *n*) threshold scheme. If *k*=*n* then all participants are required to reconstruct the secret.

C. Identity- Based Encryption(IBE)

IBE was proposed by Boneh and Franklin [3]. Identity based systems enables any party to generate a public key from a known identity value. It is a type of public key encryption in which the public key of a user is some unique information about the identity of the user. It is an important application of pairing –based cryptography.

D. Attribute-based encryption(ABE)

ABE is a public key encryption in which the secret key of a user and the cipher text are dependent upon attributes. The decryption of a cipher text is possible only if the set of attribute of the user key matches the attribute of the cipher text. In ABE data are encrypted by the owner under set of attributes. ABE has shown its promising future in fine grained access control for outsourced sensitive data[7], [8], [9], [10], [11].

III. SYSTEM AND THREAT MODELS

A. System Model

The system depicts users to collect their health data through the monitoring devices such as electrocardiogram sensors and health tracking patches as shown in Fig.2. Emergency medical technician (EMT) is a physician associated with the computing facilities mainly on mobile devices such as smart phone, tablet, or personal digital assistant. Each user is associated with one private cloud multiple private clouds are supported on same physical server. In situation of medical emergencies the health data is handled on behave of the users as the private clouds are always online. Private cloud will process the data to add security protection before it is stored to the public cloud and this is owned by amazon and google. There is a secure channel between the user and his/her private cloud and this is called bootstrap phase , example secure Wi-Fi network to negotiate long-term shared -key. After this phase is completed the user will send the health data over insecure network to private cloud residing via internet backbone. Here we are not using the mobile devices because they can disclose when sending the health data to the private cloud. There is a large body of location privacy schemes[4] and[5] in the literature.

B. Threat Model

•Avoid Private cloud is a secure cloud based environment in which the only specified client can only operate and he is fully trusted by the user to carry the health data-related computations. Public cloud is assisted to be accessible over the public network they will not delete or modify the users health data, but will attempt to compromise there privacy, Public cloud is not authorized to access any of the health data. The EMT granted access rights to the data only related to the treatment, and only when emergencies take place. EMT will also attempt to compromise data privacy by accessing the data that is not authorized and he is assumed to be rational that he/she wont access the data beyond authorization if doing so they will be caught. Finally, outside attackers can access the data though they are unauthorized.

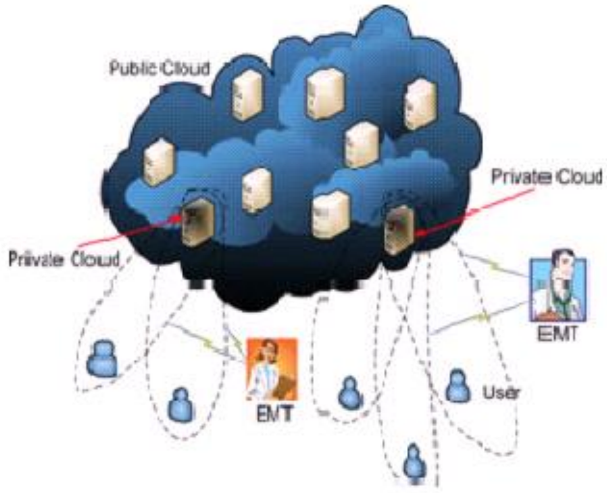

Fig.2. Cloud-assisted mobile health network

C. Security Requirements

These are the following main security requirements for practical privacy-preserving mobile healthcare systems.

1) Storage Privacy: storage on public cloud is subjected to five privacy requirements.

a) Data confidentiality: unapproved parties should not learn the content of stored data.

b) Anonymity: no distinct user can be associated with storage and retrieval process it should be anonymous.

c) Unlinkability: unauthorized parties should not be able to link multiple data files to a user. File identifiers should appear randomly and not disclose any useful information.

d) Keyword Privacy: the keyword used for search should be private because it may contain delicate information, which will prevent public cloud from incisive for desired data files.

e) Search Pattern Privacy: the searches were for the same keyword or not, and access patterns that a set of documents that contain keyword should not be revealed. This requirement is the most challenging and none of the existing SSE [1]-[6] can satisfy it. It has stronger privacy that are needed for the health data to be secured..

2) Auditability: In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requester is a legitimate EMT. Authorized parties access activities to leave cryptographic evidence.

IV. CLOUD-ASSISTED PRIVACY-PRESERVING E-HEALTH

There are two components in cloud-assisted privacy-preserving mobile healthcare system and auditable access control. The private cloud processes and stores the received health data from users. Their private cloud guarantees storage privacy and efficient retrieval and also engages bootstraping the data access and auditability scheme.

A. Storage privacy and efficient retrieval

The storage mechanism relies on secure index or SSE, such that the user can encrypt the data with additional data structures to allow for efficient search. Promising among different approaches for storage privacy is known as secure index based approach. In our environment the role of user is taken by the private cloud and the storage server in SSE is public cloud. There are practical issues that were unsolved which is addressed in this paper.

The requirement for unlinkability was not well addressed. When the identifier bear particular pattern it will be easy for the attackers to infer multiple files from the same user. The random identifiers can be easily managed. The data files are encrypted using the same key in traditional SSE. Hence the key need to be frequently updated to avoid the key wear-out. It is desirable to construct the data files such that they could be searched by the date/time of creation, besides the keyword which facilitates fast and efficient retrieval. This date/time is not strictly sensitive data and requirement for privacy can be relaxed for efficiency. Construction hides both pattern are based on oblivious RAMs and are highly inefficient because of the round complexity.

B. Pattern Hiding in Secure Index:

Private cloud construct a secure index (SI) for keyword search. The pattern hiding schema is described as for each keyword i in the keyword space.

Select a random integer m between 1 and N=|w|, where N is the number of linked list to be constructed. Integer m determines how many different linked list will contain $w_{i.}$

Then, randomly generate an array of m-1 integers between 1 and N, indicates the linked list that contained w_i beside li. The process keeps running until m distinct integers is generated. Array M (array of integers) determines the position of $w_{i.}$

In matrix Q by setting the corresponding elements to 1(otherwise 0) position of w_i is recorded. Linked list is actually constructed on array B and matrix Q.

C. Retrieving the Data Files:

Private cloud retrieve the data files upon request on behave of the users. Public cloud will obtain addresses and secret keys for all the nodes in this linked list is decrypted , Public cloud uses time tag to determine a particular file is within the time range of the request submitted by the private cloud. The files and there time tags are finally return to the private cloud .

Data Access Privacy and Auditability

The second component is the data access during emergencies where the data is requested by the EMT through the private cloud. Although we focus on the emergency access, the proposed approach is for the general data access since it is more challenging. The emergency access is based on a personal device which is subject to theft, loss or dead battery, and cannot meet the requirement of anytime anywhere accessibility. Most relevant to our data access component have followed the approach to define a set of attributes for each single data file.

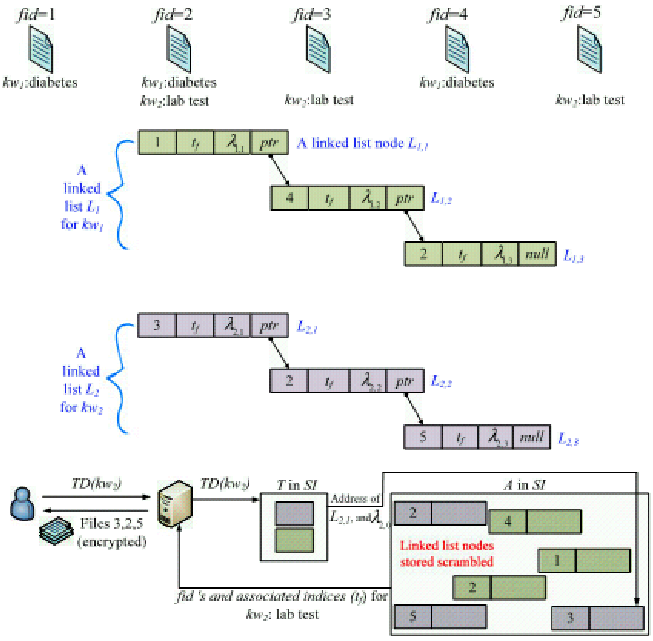

Fig.3. Example of the construction process of secure index of five files sorted by two keywords, two linked lists each created for a keyword, and a search based on the keyword "lab test."

ABE directly encrypts each file under the associated attributes or encrypted using different key which is then encrypted under the attributes. The process of constructing the secure index and using it for retrieval as shown in Fig.3. The drawback of this approach are first of all, users who needs access to which data files are not in good position this prominent feature of health data requires flexibility and professional judgment. Second the practical and challenging problem in the proposed mobile health network is that the authenticity of the attribute cannot be verified where a set of attributes which is defined for each general role that will access the data.

TABLE 1

NOTATIONS FOR EFFICIENCY ANALYSIS

S_g	Bit size of an output pseudorandom generators
S_S	Bit size of signature
S_F	Average bit size of a data file
S_{ABE}	Bit size of the ABE a secret share
S_{IBE}	Bit size of the IBE encryption of the ABE encryption key
S_{Att}	Bit size of an attribute certificate
S_l	Bit size of a linked list node
S_{LT}	Bit size of an array entry in the lookup table T
S_{Arr}	Bit size of an entry in the array A
N_P	Minimum number of parties required to generate a signature
N_A	Number of attributes used in ABE
N_f	Number of files
N_k	Number of keywords

The storage and communication overhead is defined to be any information that serves the purposes of management, security, book keeping etc., but the essential health care data or its encryption. For ease of presentation, we list in Table 1 notations of parameters that we will use in the analysis. The respective communication overheads are illustrated in Table 2.

TABLE 2

COMMUNICATION OVERHEAD FOR A SUCCESSFUL DATA ACCESS REQUEST

Communicating parties	**Overhead**	**Note**

EMT and private cloud	$N_A S_{Att} + S_s + S_{ABE} + S_{IBE} + N_P S_S$	Q and SIG(Q)
		ABE(x_d)
		IBE(D)
		N_p Partial signatures

Private cloud and public cloud	$2S_g + (N_{kn} - 1) N_{fk} S_F$	A trapdoor Redundant files for pattern hiding

V. CONCLUSION

Fine grained access control is achieved by ABE-control threshold signing scheme where the expensive ABE operation are used for only encrypting small secret values. The proposed scheme is efficient as well as scalable.

In this paper with the help of the private cloud, proposed to build privacy into mobile health system. A solution for privacy-preserving data storage by integrating a PRF based key management for unlinkability, a search and access pattern hiding scheme based on redundancy, and a secure indexing method for privacy-preserving keyword search are provided. The techniques that provide access control and auditability of the authorized parties to prevent misbehavior, by combining ABE-control threshold signing with role-based encryption are also investigated. The devise mechanism detect whether users health data have been illegally distributed, and identify possible source(s) of leakage.

REFERENCES

[1] E-J. Goh, “Secure indexes,” IACR cryptology ePrint Archieve, vol. 2003, p. 216, 2003.

[2 R. Curtmol, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” presented at the ACM Conf. Comput. Commun. Security , Alexandria, VA, USA, 2006.

[3] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001,”, SIAM J. Comput. Vol.32, no. 3, pp. 586-615, 2003.

[4] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, “CAP:A context-aware privacy protection system for location-based services”, in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2009, pp. 49-57.

[5] T. Xu and Y. Cai, “Location cloaking for safety protection of ad hoc networks”, in Proc. IEEE Conf. Comput. Commun., 2009, pp. 1994-1952.

[6] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searching on encrypted data”, in Proc. IEEE Symp. Security privacy, 2000, pp. 44-45.

[7] 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 Trans. Prallel Distib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013.

[8] M. Chase and S. S. M. Chow, “Improving privacy and security in multi authority attribute-based encryption”, in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121-130.

[9] S. S. M. Chow, “New privacy-preserving architectures for identity-/attribute-based encryption” Ph.D, dissertation, Courant Inst. Math. Sci., New York University, New York, NY, USA, 2010.

[10] V. Goyal, O. Pandy, A. Sahai, and B. Waters, “ Attribute-based encryption for fine-grained access control of encrypted data”, in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, ”Achieving secure, scalable, and fine-grained data access control in cloud computing”, presented at the IEEE Conf. Comput. Comun., San Diego, CA, USA, Mar.2010.