Advances in Computer Science and Information Technology (ACSIT)
Print ISSN : 2393-9907; Online ISSN : 2393-9915; Volume 2, Number 7; April – June, 2015 pp 97 – 102
Krishi Sanskriti Publications
http://www.krishisanskriti.org/ACSIT.html

Multi Layered Securing of Health Records using Public and Private Model in Cloud

Vijay J[1], Anitha C.L[2]

*[1]P.G.Student, Department of Computer Science, KIT
Visveswaraya Technological University, Karnataka, India
[1]vijayekrishna@gmail.com*
*[2]Assist Professor, Department of Computer Science
Kalpataru Institute of Technology, Karnataka, India
[2]clanitha@gmail.com*

Abstract: *Privacy issue is the main concern in Health care applications, dominated by the Electronic health care Systems and increased usability of cloud storage in storing health records makes the privacy a most important part in cloud storage. In this paper we propose a build in privacy using private cloud and public cloud, all the data transformation is done in private cloud and storage is done in public cloud. Different methods like pseudorandom number generator and hash functions are used for securing data files in private cloud. While retrieving health records during normal cases and emergencies auditability is maintained to avoid potential misbehavior, threshold sharing and key aggregation adds one more layer of security in hiding the privacy of health records. Searchable key encryption provides the option of searching the file without decryption of health records.*

1. INTRODUCTION

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in daily life. Services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted.

While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient.

Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information.

Outsourcing data storage and computational tasks becomes a popular trend. A wildly successful story is that the company’s total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans. TC3 has been using Amazon’s EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon’s expertise to process and analyze data faster and more efficiently. The proposed cloud assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. The private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in Fig. 1. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers (e.g., Amazon, Google).

Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud. The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.

A. Existing System

- ➢ Existing system a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys.

- Each user obtains keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online.
- An alternative is to employ a central authority CA to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority.
- Key escrow also known as a “fair” cryptosystem is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys.
- A thorough analysis of the complexity and scalability of Existing secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management

This requirement is the most challenging and none of the existing efficient SSE can satisfy it.

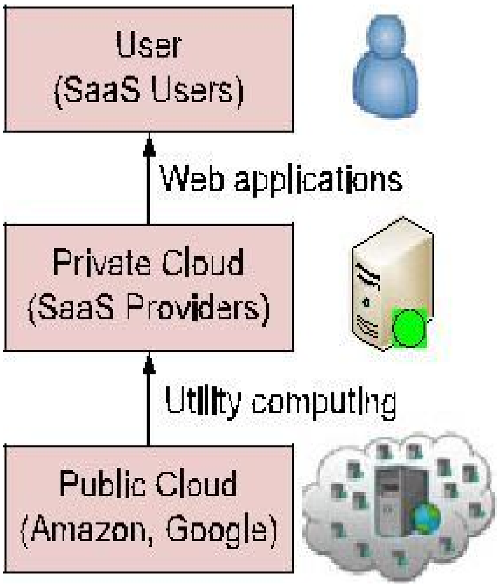

Fig. 1. SaaS service model.

Disadvantages

- Difficult for Long Term Medication. Several Kinds of Medicine Diagnosing, Frustration of missing Doses.
- Manual Insurance Climbing Patients could actually control the sharing of their sensitive PHI, especially when they are stored on a third-party server which people may not fully trust.
- Because a third-party server inside hackers can able to leak the patient’s information and security records to other peoples so this scheme is not fully trust.
- The ABE important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date.

B. Proposed System

- The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the Cloud-based data/computation outsourcing paradigm.
- Introducing the private cloud which can be considered as a service offered to mobile users.
- The result indicates that the proposed scheme is efficient as well as scalable.
- Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud.
- The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.
- The proposed pattern hiding scheme just slightly increases the computation and storage costs at the public cloud compared to the most efficient construction.

Advantages:

- Provided a thorough analysis of the complexity and scalability of proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management.
- Data Confidentiality and On-Demand Revocation. Write Access Control and Scalability and Usability.
- Proposed to build privacy into mobile health systems with the help of the private cloud.
- Provided a solution for privacy-preserving data storage by integrating a PRF based key management for unlinkability.

2. OVERVIEW

Overview provides a briefing on implementation modules and architectural design of assessing the patient health record through cloud.

A. Implementation modules:

1. Medical Information Privacy Assurance(MIPA)
2. Searchable Symmetric Encryption
3. Identity-Based Encryption
4. Attribute-Based Encryption
5. Security Requirements

Medical Information Privacy Assurance (MIPA)

Some early works on privacy protection for e-health data concentrate on the framework design, including the demonstration of the significance of privacy for e-health systems, the authentication based on existing wireless infrastructure, the role-based approach for access restrictions, etc. In particular, identity based encryption (IBE) has been used for enforcing simple role-based cryptographic access control. Among the earliest efforts on e-health privacy, Medical Information Privacy Assurance (MIPA) pointed out the importance and unique challenges of medical information privacy, and the devastating privacy breach facts that resulted from insufficient supporting technology. MIPA was one of the first few projects that sought to develop privacy technology and privacy-protecting infrastructures to facilitate the development of a health information system, in which individuals can actively protect their personal information. Privacy-preserving health data storage is studied by Sun et al. , where patients encrypt their own health data and store it on a third party server.

Searchable Symmetric Encryption

Searchable symmetric encryption (SSE) allows data owners to store encrypted documents on re-mote server, which is modeled as honest but curious party, and simultaneously provides a way to search over the encrypted documents. More importantly, neither the operation of outsourcing nor keyword searching would result in any information leakage to any party other than the data owner, thus achieving a sound guarantee of privacy.

- **KeyGen (s)**: This function is used by the users to generate keys to initialize the scheme. It takes the security parameter s and outputs a secret key K.
- **BuildIdx (D, K)**: The user runs 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 , through which document can be searchable while remaining encrypted.
- **Trapdoor (K, w)**: The user runs this function to compute a trapdoor for a keyword w, enabling searching for this keyword. A trapdoor T_w can also be interpreted as a proxy for w in order to hide the real meaning of w. Therefore, T_w should leak the information about w as little as possible. The function takes the 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. Due to the use of the trapdoor, the server is able to carry out the specific query without knowing the real keyword. The function takes the built secure index I and the trapdoor T_w, and outputs the identifiers of files which contains keyword w.

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. For (k, n) threshold secret sharing, a piece of information I is divided into n pieces I_1 , . . . , I_n , such that knowledge of any k or more of these I_i (i €[1, n]) pieces can recover I , while knowledge of (k − 1) or fewer pieces keeps I completely un-determined.. Specifically, for the secret I = a_0 is in a group G, randomly pick a (k − 1) degree polynomial.

Identity-Based Encryption

A practical IBE scheme in the random oracle model was proposed by Boneh and Franklin [7]. Identity-based systems allow any party to generate a public key from a known identity value, for example, the string “alice@xyz.com” for Alice. IBE makes it possible for any party to encrypt message with no prior distribution of keys between individuals. It is an important application of the pairing based cryptography.

Attribute-Based Encryption

ABE has shown its promising future in fine-grained access control for outsourced sensitive data [9]. Typically, data are encrypted by the owner under a set of attributes. The parties accessing the data are assigned access structures by the owner and can decrypt the data only if the access structures match the data attributes.

3. PROBLEM DEFINITION

The main entities involved systems are depicted in Fig. 2 Users collect their health data through the monitoring devices worn or carried, e.g., electrocardiogram sensors and health tracking patches. Emergency medical technician (EMT) is a physician who performs emergency treatment. By user and EMT, referred to the person and the associated computing facilities. The computing facilities are mainly mobile devices carried around such as Smartphone, tablet, or personal digital assistant.

A. System Model

Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server Fig. 3. Private clouds are always online and available to handle health data on behalf of the users. This can be very desirable in situations like medical emergencies.

The private cloud will process the data to add security protection before it is stored on the public cloud. Public cloud is the cloud infrastructure owned by the cloud providers such as Amazon and Google which offers massive storage and rich computational resource.

Assuming that at the bootstrap phase, there is a secure channel between the user and his/her private cloud, e.g., secure home Wi-Fi network, to negotiate a long-term shared-key. After the bootstrap phase, the user will send health data over insecure network to the private cloud residing via the Internet backbone.

B. Threat Model

The private cloud is fully trusted by the user to carry out health data-related computations. Public cloud is assumed to be honest-but-curious, in that they will not delete or modify users’ health data, but will attempt to compromise their privacy. Public cloud is not authorized to access any of the health data Fig. 4.

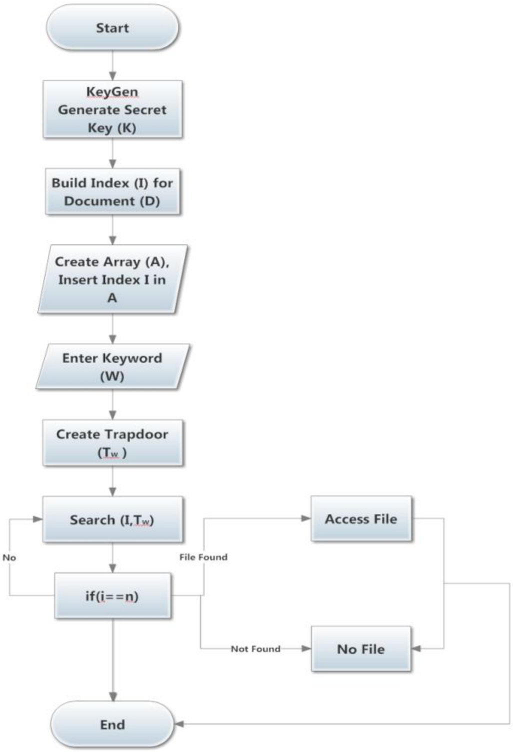

Fig. 2. Searchable symmetric encryption

The EMT is granted access rights to the data only pertinent to the treatment, and only when emergencies take place. The EMT will also attempt to compromise data privacy by accessing the data he/she is not authorized to. The EMT is assumed to be rational in the sense that he/she will not access the data beyond authorization if doing so is doomed to be caught. Finally, outside attackers will maliciously drop users packets, and access users' data though they are unauthorized.

Security Requirements

The following main security requirements are needed for practical privacy-preserving mobile healthcare systems,

1) **Storage Privacy:** Storage on the public cloud is subject to five privacy requirements.

a) Data confidentiality: unauthorized parties (e.g., public cloud and outside attackers) should not learn the content of the stored data.

b) Anonymity: no particular user can be associated with the storage and retrieval process, i.e., these processes should be anonymous.

c) Unlinkability: unauthorized parties should not be able to link multiple data files to profile a user. It indicates that the file identifiers should appear random and leak no useful information.

d) Keyword privacy: the keyword used for search should remain confidential because it may contain sensitive information, which will prevent the public cloud from searching for the desired data files.

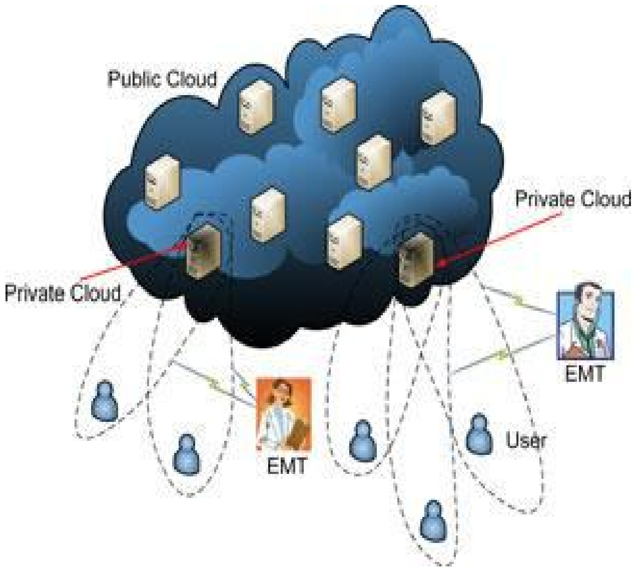

Fig. 3 Cloud-assisted mobile health network.

e) Search pattern privacy: whether the searches were for the same keyword or not, and the access pattern, i.e., the set of documents that contain a key-word should not be revealed. This requirement is the most challenging and none of the existing efficient SSE can satisfy it. It represents stronger privacy which is particularly needed for highly sensitive applications like health data networks.

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. The required authorization to be fine-grained and authorized parties access activities to leave cryptographic evidence.

C. Cloud assisted Privacy preserving eHealth

Cloud assisted privacy preserving mobile healthcare system consists of two components: **searchable encryption** and auditable **access control**. Upon receiving the health data from users, the private cloud processes and stores it on public cloud such that storage privacy and efficient retrieval can be guaranteed. Next, the private cloud engages in the bootstrapping of data access and auditability scheme with users so that it can later act on the users' behalf to exercise access control and auditing on authorized parties.

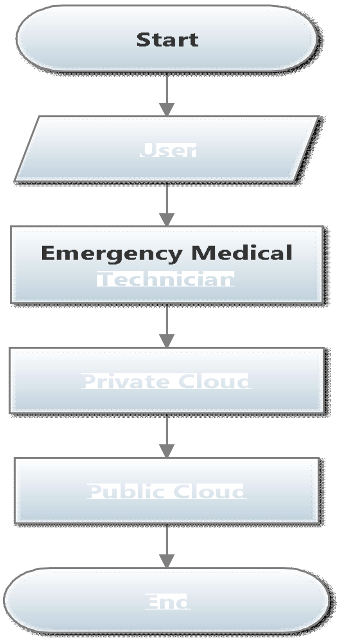

Fig. 4 System model.

Storage Privacy and Efficient Retrieval

The first component is storage privacy for the health data. Here storage mechanism relies on secure index or SSE, so that the user can encrypt the data with additional data structures to allow for efficient search. It has been proven that the secure index-based approach is promising among different approaches for storage privacy. In this environment, the private cloud takes the role of user, and the public cloud is the storage server in SSE.

1)The unlinkability requirement was not well addressed. None of the above works mentioned how to construct the file identifiers. If the identifiers bear certain pattern, it will be easy for the attackers to infer that multiple files are from a same user. Clearly, the need of identifiers that appear random yet can be easily managed.

2)In traditional SSE, all stored data files are encrypted using the same key. This is not a sound security design since the more usage of key, the more information the attackers can obtain to break the key. Therefore it needs to update the key frequently enough to avoid the key wear-out.

3)To facilitate fast and efficient retrieval, it is desirable to construct the data files such that they could be searched by the date/time of creation, besides the keywords. This is particularly useful in emergencies where the search can be narrowed down to the most helpful data. Searching based on date/time should be treated differently from keywords since date/time is not strictly sensitive information and the privacy requirement can be relaxed for efficiency.

4)None of the existing relevant works [7] could hide the search or access pattern as discussed before.. These constructions are based on oblivious RAMs and are highly inefficient due the round complexity.

Data Access Privacy and Auditability

The second component is the data access during emergencies where the EMT requests data through the private cloud. The proposed approach is for the general data access, although focus on the emergency access since it is more challenging. The emergency access supported by Sun et al. [7] is based on a personal device which is subject to theft, loss, or dead battery, and cannot meet the requirement of anytime anywhere accessibility.

Existing papers, most relevant on data access component that followed the approach to define a set of attributes for each single data file [9]. Each file is then directly encrypted under the associated attributes by ABE [9] or encrypted by a different key which is in turn encrypted under the attributes by ABE. There are some significant drawbacks of this approach.

First of all, users (or data owners) are not in a good position to determine who needs access to which data files. This is one of the most prominent features of health data access which requires flexibility and professional judgment. Second, the authenticity of the attributes cannot be verified which is a very practical problem and highly challenging in the proposed mobile health networks, where a set of attributes is defined for each general role (e.g., primary physician, EMT, and insurance provider) that will access the data. For example, a user would like to grant data access to someone who is a pediatrician, has more than ten years experience, works in the Bay Area, and accepts the Blue Cross and Blue Shield or IGNACIO insurance plan. How does the private cloud verify, at the time of data access, that the person indeed has the attributes he/she claims? Third, using the ABE-based access control alone cannot audit who has accessed which data. ABE serves as a gatekeeper to prevent unauthorized parties from decrypting the data.

However, it does not provide any mechanism for auditability, i.e., to record and prove that an authorized party has accessed certain data. Without auditability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data which will be discussed in future research issues. Furthermore, the use of ABE, the user (and his/her primary physician) will have no clue about whether an authorized party has properly accessed the data without auditability.

To overcome these difficulties, A combine thresh-old signature with ABE-based access control is proposed Fig.5. A (k, n) threshold signature guarantees that a valid signature on a message can be generated as long as there are k valid signature shares. If user consider the value n as 5 representing the private cloud, the primary physician, the EMT, the specialists (e.g., pediatrician and urologist), and the insurance provider. The private cloud and primary physician are fully trusted by the user. Let k be value 2 such that any not fully trusted party must perform the threshold signing with either fully trusted party.

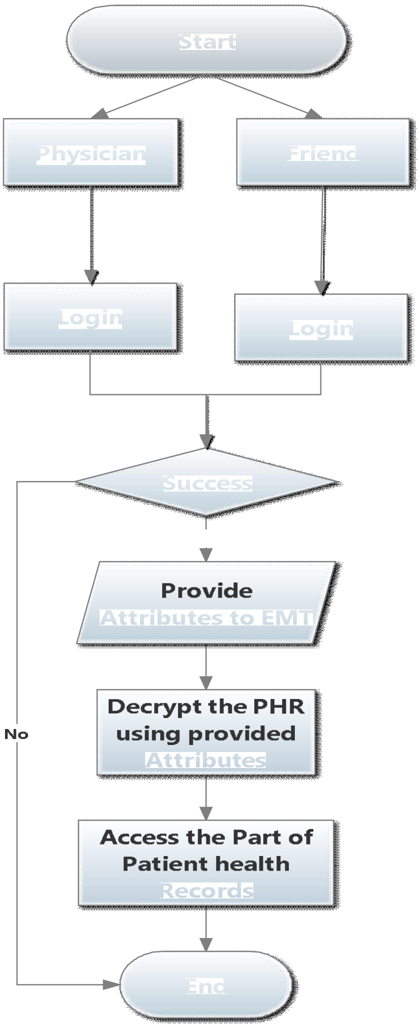

Fig.5 Threshold Sharing

CONCLUSION

roposed system is to build privacy into mobile health systems with the help of the private cloud. Here provided 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. The investigated techniques that provide access control (in both normal and emergency cases) and auditability of the authorized parties to prevent misbehavior, by combining ABE controlled threshold signing with role based encryption has been introduced. As future work, plan to devise mechanisms that can detect whether users health data have been illegally distributed, and identify possible source(s) of leakage.

REFERENCES

[1] L. Zhang, G. J. Ahn, and B. T. Chu, “A role-based delegation framework for healthcare information systems,” in 7th ACM Symp. Access Control Models Technol., Monterey, CA, USA, 2002, pp. 125–134.

[2] L. Zhang, G. J. Ahn, and B. T. Chu, “A role-based delegation framework for healthcare information systems,” in 7th ACM Symp. Access Control Models Technol., Monterey, CA, USA, 2002, pp. 125–134.

[3] L. Zhang, G. J. Ahn, and B. T. Chu, “A rule-based framework for role-based delegation and revocation,” ACM Trans. Inf. Syst. Security, vol. 6, no. 3, pp. 404–441, 2003.

[4] J. Sun, X. Zhu, C. Zhang, and Y. Fang, “HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare,” in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[5] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searching on encrypted data,” in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[6] M. Katzarova and A. Simpson, “Delegation in a distributed healthcare context: A survey of current approaches,” in Proc. 9th Int. Conf. Inform. Security, 2006, pp. 517–529.

[7] 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.

[8] D. Song, D.Wagner, and A. Perrig, “Practical techniques for searching on encrypted data,” in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled

[10] encryption: Ensuring privacy of electronicmedical records,” in *Proc. ACM Workshop Cloud Comput. Security*, 2009, pp. 103–114.

[11] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, “Keyaggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 99, no. PrePrints, p.1, 2013. Available: http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.112