IJDCST @Dec-2015, Issue- V-3, I-8, SW-06
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Mobile-Access of Health Data supported by Cloud with Attribute-based Encryption and Auditability

Surekha Lathan Leburi[1], B. Trivikrama Rao[2]
[1]M.Tech (CSE), Usha Rama College of Engineering and Technology, A.P., India.
[2]Asst Professor, Dept. of Information Technology, Usha Rama College of Engineering and Technology, A.P., India.

Abstract — Privacy issues like restricting the adoption of electronic healthcare systems and the wild success of cloud service models motivated us to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Specifically, we propose to integrate key management from pseudorandom number generator for unlinkability, a secure indexing method for privacy preserving keyword search which hides both search and access patterns based on redundancy, and integrate the concept of attribute-based encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.

Keywords — Access control, auditability, eHealth, privacy.

I. INTRODUCTION

Swift and accurate 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 our 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. According to the government website [1], around 8 million patients' health information was leaked in the past two years. 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 as we enter the cloud computing era. 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.

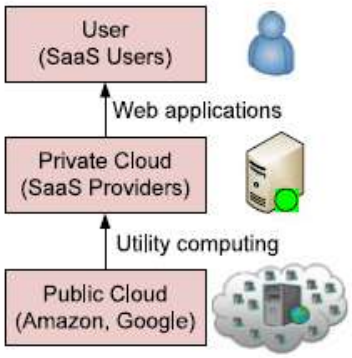

Figure 1 SaaS service model.

We introduce 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.

II. PROBLEM STATEMENT

System Model

The main entities involved in our system are shown 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, we refer 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.

Figure 2: Cloud-assisted mobile health network

Each user is associated with one private cloud. Multiple private clouds are supported on the same physical server. 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. We assume 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. Note that, we do not focus on the location privacy of mobile users which can be leaked when sending health data to the private cloud. There is a large body of location privacy schemes [1], [2] in the literature.

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.

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 to.

Security Requirements

In this paper, we strive to meet the following main security requirements 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.

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 keyword [3], should not be revealed. This requirement is the most challenging and none of the existing efficient SSE [4]-[5] can satisfy it. It represents stronger privacy which is particularly needed for highly sensitive applications like health data networks.

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. We require authorization to be fine-grained and authorized parties' access activities to leave a cryptographic evidence.

To deal with the security issue in [6], instead of using the system unique public key (generated by the unique master key) to encrypt data, our scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevents the certificate authority in our scheme from decrypting the ciphertexts.

III. CLOUD-ASSISTED PRIVACY-PRESERVING EHEALTH

Our 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.

Storage Privacy and Efficient Retrieval

The first component is storage privacy for the health data. Our 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 shown [7] that the secure index-based approach is promising among different approaches for storage privacy. In our environment, the private cloud takes the role of user, and the public cloud is the storage server in SSE.

Sun et al. [8] shows the feasibility of the secure index for health data storage privacy. Their approach followed the SSE of Curtmola et al. [9] which uses a linked-list data structure. However, there are practical issues that were unsolved which we will address in this paper.

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, we need 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 we use a key, the more information the attackers can obtain to break the key. We therefore need 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 could hide the search or access pattern as discussed before. The only SSE schemes that hide both patterns are proposed by Goldreich and Ostrovsky. These constructions are based on oblivious RAMs and are highly inefficient due the round complexity.

We take a heuristic approach instead of hiding the search and access patterns instead of relying on relatively heavy cryptographic techniques. Our proposed pattern hiding scheme just slightly increases the computation and storage costs at the public cloud compared to the most efficient construction [15].

IV. RELATED WORK

Some early works on privacy protection for e-health data concentrate on the framework design [2]–[6], 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) [7] has been used [3] for enforcing simple role-based cryptographic access control. Among the earliest efforts on e-health privacy, Medical Information Privacy Assurance (MIPA) [4] 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. We followed our line of research [10]–[12] with other collaborators and summarized the security requirements for e-health systems in [10], [12].

Privacy-preserving health data storage is studied by Sun et al. [11], where patients encrypt their own health data and store it on a third-party server. This work and Searchable Symmetric Encryption (SSE) schemes are most relevant to this paper. Another line of research closely related to this study focuses on cloud-based secure storage and keyword search. The detailed differences will be described later. The proposed cloud-assisted health data storage addresses the challenges that have not been tackled in the previously stated papers.

There is also a large body of research works on privacy-preserving authentication, data access, and delegation of access rights in e-health systems [5], [6], while [11] are most related to our proposed research.

Lee and Lee proposed a cryptographic key management solution for health data privacy and security. In their solution, the trusted server is able to access the health data at any time, which could be a privacy threat. The work of Tan et al. is a technical realization of the role-based approach proposed in [3]. The scheme that failed to achieve privacy protection in the storage server learns which records are from which patient in order to return the results to a querying doctor.

Benaloh et al. proposed the concept of patient-controlled encryption (PCE) such that health-related data are decomposed into a hierarchy of smaller piece of information which will be encrypted using the key which is under the patients' control. They provided a symmetric-key PCE for fixed hierarchy, a public-key PCE for fixed hierarchy, and a symmetric-key PCE for flexible hierarchy from RSA. The first public-key PCE for flexible hierarchy from pairings is proposed by Chu et al. The system of Li et al. utilizes multiauthority attribute-based encryption (ABE) proposed by Chase and Chow for fine-grained access control. Their system allows break-glass access via the use of "emergency" attributes. However, it is not clear who will take on the role of issuing such a powerful decryption key corresponding to this attribute in practice.

The backup mechanisms in [11] for emergency access rely on someone or something the patient trusts whose availability cannot be guaranteed at all times. Moreover, the storage privacy proposed in [11] is a weaker form of privacy because it does not hide search and access patterns. The previously stated research works failed to address the challenges in data privacy, we aim to tackle in this paper.

Finally, we also remark that there are other cryptographic mechanisms for privacy-preserving access of general data stored in a cloud environment.

V. CONCLUSION

In this paper, we proposed to build privacy into mobile health systems with the help of the private cloud. We 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. We also 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. As future work, we plan to devise mechanisms that can detect whether users' health data have been illegally distributed, and identify possible source(s) of leakage (i.e., the authorized party that did it).

REFERENCES

[1] U.S. Department of Health & Human Service, "Breaches Affecting 500 or More Individuals," (2001). [Online]. Available: http://www.hhs.gov/ocr/ privacy/hipaa/administrative/breachnotificationr ule/breachtool.html

[2] P. Ray and J.Wimalasiri, "The need for technical solutions formaintaining the privacy of EHR," in Proc. IEEE 28th Annu. Int. Conf., New York City, NY, USA, Sep. 2006, pp. 4686–4689.

[3] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague, Czech Republic, 2003.

[4] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.

[5] 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.

[6] L. Zhang, G. J. Ahn, and B. T. Chu, "A rule-based framework for rolebased delegation and revocation,"

ACM Trans. Inf. Syst. Security, vol. 6, no. 3, pp. 404–441, 2003.
[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] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, Sep. 2010.
[9] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," in Proc. IEEE Global Telecommun.
Conf., Dec. 2010, pp. 1–6.
[10] J. Sun, X. Zhu, and Y. Fang, "Privacy and emergency response in ehealthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.
[11] J. Sun, X. Zhu, C. Zhang, andY. 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.
[12] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," in Proc. IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.