International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Secure Access of Health Data through Mobiles in Cloud

[1] P. Prabha &[2] R.Suresh

[1]M.Tech Student(Branch (CSE) Department of CSE ,CREC,Tirupathi,JNTU Anathapuram, A.P ,India.
Email id:- prabharoyal17@gmail.com.

[2]Associate Professor and HOD of CSE CREC,Tirupathi,JNTU Anathapuram, A.P ,India.
Email id: ramsuri42@gmail.com.

Abstract—
Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose 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 audit ability for misusing health data. Specifically, we propose to integrate key management from pseudorandom number generator for unlink ability, 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 audit ability to prevent potential misbehavior, in both normal and emergency cases.

Keywords— Access control; auditability; eHealth; privacy

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 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 Auditable Cloud-Assisted Access of Encrypted Health 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.

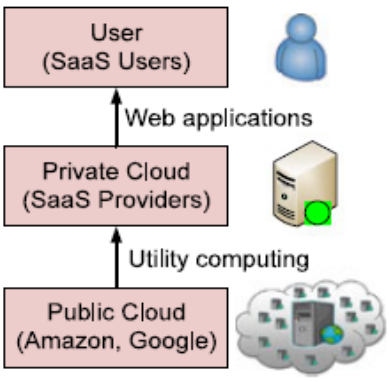

Fig. 1. SaaS service model.

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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

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.

2. EXISTING SYSTEM

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, 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.

DISADVANTAGES OF EXISTING SYSTEM:

- Privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short.
- The storage privacy in the existing system is a weaker form of privacy because it does not hide search and access patterns.
- There is a shortage of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information.

3. PROPOSED SYSTEM

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. 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.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Fig 2: Proposed System Architecture

ADVANTAGES OF PREPOSED 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.
- The proposed system has other cryptographic mechanisms for privacy-preserving access of general data stored in a cloud environment.
- The proposed solutions are built on the SaaS model of cloud computing. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers.

4. IMPLEMENTATION

The system is proposed to have the following modules along with functional requirements:

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:

SSE allows data owners to store encrypted documents on remote server, which is modeled as honest-but-curious party, and simultaneously provides away to search over the encrypted documents.

Key Gen(*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*.

Build Idx (*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 *Tw* can also be interpreted as a proxy for *w* in order to hide the real meaning of *w*. Therefore, *Tw* 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 *Tw* .

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015
Available at http://internationaljournalofresearch.org

Search(*I, Tw*): 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 *Tw* , and outputs the identifiers of files which contains keyword *w*.

Identity-Based Encryption

A practical IBE scheme in the random oracle model was proposed by Bone h and Franklin. 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. 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.

Security Requirements:

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) *Unlink ability:* 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, 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.

2) *Audit ability:* 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 cryptographic evidence.

5 CONCLUSIONS

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 unlink ability, 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].

[2] P. Ray and J.Wimalasiri, "The need for technical solutions for maintaining 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.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, Security and Privacy for Mobile Healthcare (m-Health) Systems, in Handbook on Securing Cyber-Physical Infrastructure, S. Das, K. Kant, and N. Zhang, Eds. Amsterdam, The Netherlands: Elsevier, 2011.

[14] E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[15] R. Curtmola, 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.

[16] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Security, 2005, pp. 442–455.

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

[18] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," J. ACM, vol. 43, pp. 431–473, 1996.

[1] P. Prabha , M.Tech Student(Branch (CSE) Department of CSE ,CREC,Tirupathi,JNTU Anathapuram, A.P ,India. Email id: MailId:-prabharoyal17@gmail.com., Her current interests include Computer Networks and