International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

PRIVACY PRESERVING IN HEALTH RECORDS

DLK.Vijaybharath,
Department of Information Technology,
Velammal Insitute Of Technology,Chennai.

S.Arvind,
B.Tech Student,
Department of Information Technology,
Velammal Insitute Of Technology,Chennai.

R.Rohith,
B.Tech Student,
Department of Information Technology,
Velammal Insitute Of Technology,Chennai.

Abstract: In Distributed Cloud computing provides a technique to break up a problem so that we can have a whole bunch of computers work on it at the same time in Cloud Computing. Health records enable the global availability of medical data. This has numerous benefits for the quality of offered services. However, privacy concerns may arise as now both the patient's medical history as well as the doctor's activities can be tracked. In this paper, We proposed, a novel authorized accessible privacy model (AAPM). Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Based on AAPM, a patient self-controllable multilevel privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels of security and privacy requirement for the patients. The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

Keywords: Distributed Cloud computing, Health Insurance, authentication

I.INTRODUCTION

Distributed m-healthcare cloud computing systems have been increasingly adopted worldwide including the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality medical treatment. In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering.

As to the security facet, one of the main issues is access control of patients' personal health information, namely it is only the authorized physicians or institutions that can recover the patients' personal health information during the data sharing in the distributed m-healthcare cloud computing system. In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions. There have emerged various research results focusing on them. A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE).

A rendezvous-based access control method provides access privilege if and only if the patient and the physician meet in the physical world. Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing. However, it mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system. Moreover, it is not enough for to only guarantee the data confidentiality of the patient's personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients' data confidentiality and identity privacy in the distributed m-

healthcare cloud computing scenario under the malicious model was left untouched.

II.EXISTING SYSTEM

In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering

In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed m-healthcare cloud computing systems, which part of the patients' personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions

DISADVANTAGE

- Lack of data confidentiality
- Security and privacy of patient is not considered

III.PROPOSED SYSTEM

The main contributions of this paper are summarized as follows.

- A novel authorized accessible privacy model (AAPM) for the multi-level privacy-preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates.
- Based on AAPM, a patient self-controllable multilevel privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels of security and privacy requirement for the patients.
- The formal security proof and simulation results show that our scheme far outperforms the previous constructions in terms of privacy-preserving capability, computational, communication and storage overhead.

ADVANTAGE

- Simultaneously achieving data confidentiality and identity privacy with high efficiency

IV.MODULES

1. Network Model.
2. Attribute Based Designated Verifier Signature Scheme
3. Adversary Models
4. PSMPA Design
5. Attribute-based encryption (ABE)

Network Model

The basic e-healthcare system mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers. The patient's personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment. We further illustrate the unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation.

There are three distributed healthcare providers A; B; C and the medical research institution D, where Dr. Brown, Dr. Black, Dr. Green and Prof. White are working respectively. Each of them possesses its own cloud server. It is assumed that patient P registers at hospital A, all her/his personal health information is stored in hospital A's cloud server, and Dr. Brown is one of his directly authorized physicians. For medical consultation or other research purposes in cooperation with hospitals B; C and medical research institution D, it is required for Dr. Brown to generate three indistinguishable transcript simulations of patient P's personal health information and share them among the distributed cloud servers of the hospitals B;C and medical research institution D.

Attribute Based Designated Verifier Signature Scheme

We propose a patient self-controllable and multi-level privacy-preserving cooperative authentication scheme based on ADVS to realize three levels of security and privacy requirement in distributed m-healthcare cloud computing system which mainly consists of the following five algorithms:

- Setup
- Key Extraction
- Sign
- Verify and
- Transcript Simulation Generation.

Adversary Models

Unforgeability: In an attribute based designated verifier signature scheme, as to Unforgeability, we mean that the adversary wants to forge a signature w.r.t an unsatisfied verifier's specific access structure. The definition of Unforgeability allows an adversary not to generate an effective signature

Anonymity for the Patient: To guarantee a strong privacy for the patient, the signature reveals nothing about the identity of the patient except the information explicitly revealed.

PSMPA Design

In this section, we give a design of the proposed PSMPA to implement AAPM introduced previously, realizing three different levels of security and privacy requirements

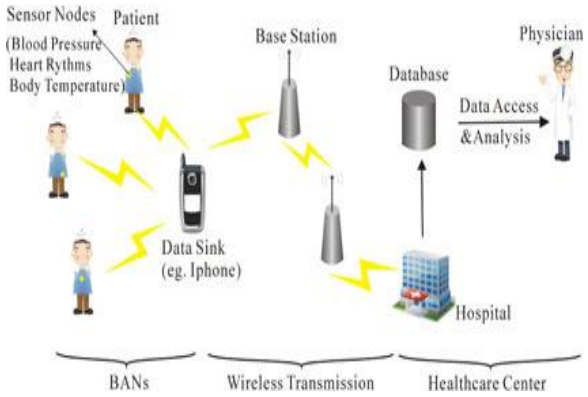
- Key extract
- Sign
- Verify

In our proposed PSMPA, for directly authorized physicians, performing the Verify algorithm allows them to both decipher the patient's identity using the private key of the patient's registered local healthcare provider and recover the patient's personal health information m using the authorized attribute private key. (i.e., although other physicians working in the patient are registered, they cannot decipher the personal health information. Therefore, the unlink ability between the patient identity and his personal health information can still be preserved). For indirectly authorized physicians working in other hospitals or institutions, only the identically distributed and indistinguishable transcript is delivered (i.e., from which only the blinded identity randomized by the protected session secret can be derived) and they cannot get the patient's authentic identity since they fail in recovering from without. For unauthorized persons (adversaries), nothing could be obtained. It is also observed that for the latter two categories, different signatures generated by the same patient cannot even be linkable without knowing his real identity.

Attribute-based encryption (ABE)

ABE is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

V.ARCHITECTURE



VI.CONCLUSION

In this paper, a novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.

VII.REFERENCE

[1] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare recordsineurope,"Int.J.Med.Inf.,vol.52,no.1,pp.105–115,1998.

[2] F. W. Dillema and S. Lupetti, "Rendezvous-based access control for medical records in the pre-hospital environment," in Proc. 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Support Healthcare Assisted Living, 2007, pp. 1–6.

[3] V. Goyal, O. Pandey, 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.

[4] M. D. N. Huda, N. Sonehara, and S. Yamada, "A privacy management architecture for patient-controlled personal health record system," J. Eng. Sci. Technol., vol. 4, no. 2, pp. 154–170, 2009.