International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 6.111

Novel Authorized Accessible Privacy Model in Distributed m-Healthcare Cloud Computing System

Geetha S, PG Student, Dept of Computer Science and Engg, Alvas Institute of Engineering and Technology, Moodbidri

Manjunath Kotari, Senior Associate Professor & Head of Department CSE, Alvas Institute of Engineering and Technology, Moodbidri

Abstract: ***Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.***

Keywords: Authentication, access control, security and privacy, distributed cloud computing, m-healthcare system

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.

In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. As is described in Fig. 1, in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient's

personal health information and verify the patient's identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes (i.e., since they are not authorized by the patients, we use the term 'indirectly authorized' instead). They can only access the personal health information, but not the patient's identity. For the unauthorized persons with red labels, nothing could be obtained. By extending the techniques of attribute based access control and designated verifier signatures (DVS) on de-identified health information, we realize three different levels of privacy-preserving requirement mentioned above. The main contributions of this paper are summarized as follows.

(1) 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.

(2) 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.

(3) 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.

II. Related Works

There exist a series of constructions for authorized access control of patients' personal health information. As we discussed in the previous section, they mainly study the issue of data confidentiality in the central cloud computing architecture, while leaving the challenging problem of realizing different security and privacy-preserving levels with respect to (w.r.t.) kinds of physicians accessing distributed cloud servers unsolved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy-preserving techniques. Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary. Sun et al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge. Lu et al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. Misic and Misic suggested patients have to consent to treatment and be alerted every time when associated physicians access their records [31], [32]. Riedl et al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE). Slamanig and Stingl integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a central m-healthcare cloud server. Schechter et al. proposed an anonymous authentication of membership in dynamic groups. However, since the anonymous authentication mentioned above are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed. In this paper, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed Fig. 1. Multiple security and privacy levels in m-Healthcare cloud computing system.

III.NETWORK MODEL

The basic e-healthcare system illustrated in Fig. 2 mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers [1], [2].

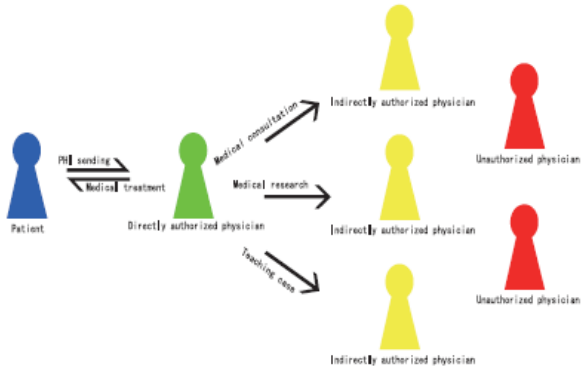

Figure 1: Multiple security and privacy levels in m-Healthcare cloud computing system

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. A typical architecture of a distributed m-healthcare cloud computing system is shown in Fig. 3.

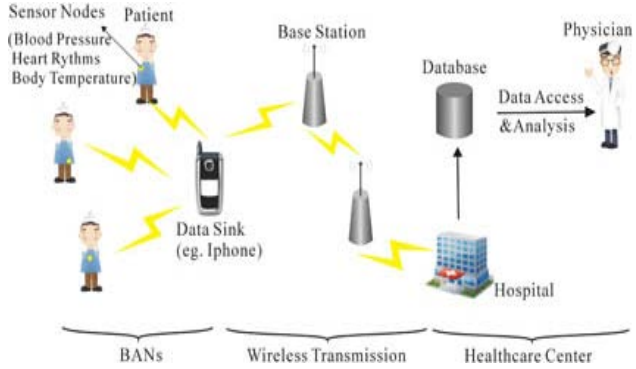

Figure 2: An basic architecture of the e-health system

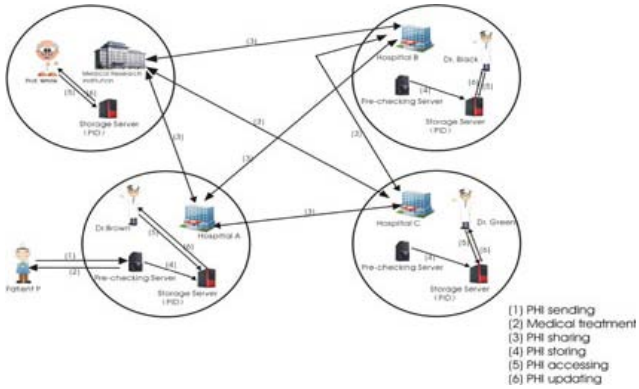

Figure 3: An overview of our distributed m healthcare cloud computing system

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.

IV. 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.

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 researches 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.

MAJOR DRAWBACKS OF THE EXISTING SYSTEM

- Security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering is not ensured
- Issue with Access control of patients' personal health information.
- 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.

- 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 mode.

V. PROPOSED SYSTEM

In this project, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

Last but not least, it is noticed that our construction essentially differs from the trivial combination of attribute based encryption and designated verifier signature. As the simulation results illustrate, we simultaneously achieve the functionalities of both access control for personal health information and anonymous authentication for patients with significantly less overhead than the trivial combination of the two building blocks above. Therefore, our PSMPA far outperforms the previous schemes, in efficiently realizing access control of patients' personal health information and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing systems.

MAJOR ADVANTAGES OF THE PROPOSED SYSTEM

- Enhanced Security and Anonymity level by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients' attribute.
- Patient encrypts his own PHI under a specified access policy rather than assign each physician a secret key.
- Our PSMPA far outperforms the previous schemes, in efficiently realizing access control of patients' personal health information and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing systems.

VI. AUTHORIZED ACCESSIBLE PRIVACY MODEL

In this section, we propose a novel authorized accessible privacy model for distributed m-healthcare cloud computing systems which consists of the following two components: an attribute based designated verifier signature scheme (ADVS) and the corresponding adversary model.

6.1Attribute 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. Denote the universe of attributes as U.

We say an attribute set v satisfies a specific access structure A if and only A(w)=1 where w is chosen from U. The algorithms are defined as follows.

Setup: On input 1l, where l is the security parameter, this algorithm outputs public parameters and y as the master key for the central attribute authority.

Key Extract: Suppose that a physician requests an attribute set wD E U. The attribute authority computes skD for him if he is eligible to be issued with skD for these attributes.

Sign: A deterministic algorithm that uses the patient's private key skP , the uniform public key pkD of the healthcare provider where the physicians work and a message m to generate a signature s.

Verify: Assume a physician wants to verify a signature s with an access structure A and possesses a subset of attributes vJ vD satisfying A(wj)=1, a deterministic verification algorithm can be operated. Upon obtaining a signature s, he takes as input his attribute private key skD and the patient's public key pkP , then returns the message m and True if the signature is correct, or ? Otherwise.

Transcript Simulation Generation: We require that the directly authorized physicians who hold the authorized private key skD can always produce identically distributed transcripts indistinguishable from the original protocol via the Transcript Simulation algorithm.

Due to the fact that the Transcript Simulation algorithm can generate identically distributed transcripts indistinguishable from the original signature s, the patient's identity can be well protected from the indirectly authorized physicians for whom only the transcripts are delivered. In addition to the main algorithms described above, we also require the following properties.

6.2 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 with an access structure A for the verifiers if he has not queried the private key for v* or any superset of it such that A(w)=1, or he has not queried the signature on the forged message m* with an access structure A* such that A(w)=1. We provide a formal definition of existential unforgeability of PSMPA under a chosen message attack. It is defined using the following game between an adversary A and a simulator B.

Initial Phase: A chooses and outputs a challenge access structure A* that will be included in the forged signature.

Setup Phase: After receiving the challenge access structure A* B selects a proper security parameter 1^l, runs the Setup algorithm to generate key pairs (sk, pk), sends pk and other public parameters to the adversary A and remains the private key sk secretly.

Query Phase: After receiving the public parameters, A can operate a polynomially bounded number of queries on vD and (m, A*) to the key extraction oracle and the signing oracle between the patient and the corresponding physician at most qk; qs times respectively. B answers with skD and s as the responses. As to the verifying queries, A can request a signature verification on a pair (m*, s*) between the patient and the directly authorized physicians at most qv times. In respond, B outputs True if it is correct, or ? Otherwise.

Forgery Phase: Finally, the adversary A outputs a signature s* on messages m* with respect to A* which is the challenge access structure sent to B during the initial phase.

The forged signature must satisfy the following three properties.

(1) A did not send queries of the attribute set vD satisfying A(W)=1 to the key extraction oracle.

(2) (m*, A*) has not been queried to the signing oracle between the patient P and the corresponding physician D.

(3) s is a valid signature of the message m* between the patient P and the corresponding physician D.

VII. CONCLUSIONS

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

REFERENCES

[1] L. Gatzoulis and I. Iakovidis, "Wearable and portable E-health systems," IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, Sep.-Oct. 2007.

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

[3] E. Villalba, M. T. Arredondo, S. Guillen, and E. Hoyo-Barbolla, "A new solution for a heart failure monitoring system based on wearable and information technologies in," in Proc. Int. Workshop Wearable Implantable Body Sens. Netw., Apr. 2006, pp. 150–153.

[4] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card," Comput. Netw., vol. 49, no. 4, pp. 535–540, 2005.

[5] 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.

[6] S. Schechter, T. Parnell, and A. Hartemink, "Anonymous authentication of membership in dynamic groups in," in Proc. 3rd Int. Conf. Financial Cryptography, 1999, pp. 184–195.

[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner, and J. Thierry, "Anonymity and application privacy in context of mobile computing in eHealth," in Mobile Response, New York, NY, USA: Springer, 2009 pp. 148–157.

[8] J. Zhou and Z. Cao, "TIS: A threshold incentive scheme for secure and reliable data forwarding in vehicular delay tolerant networks," in Proc. IEEE Global Commun. Conf., 2012, pp. 985–990.

[9] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," in Proc. IEEE Conf. Comput. Commun., 2009, pp. 963–971.

[10] 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.

[11] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for Ehealth systems," IEEE J. Sel. Areas Commun., vol. 27, no. 4 pp. 365–378, May 2009.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. 31st Int. Conf. Distrib. Comput. Syst., 2011, pp. 373–382.

[14] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L. M. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1325–1337, Oct. 2008.

[15] J. Zhou and M. He, "An improved distributed key management scheme in wireless sensor networks," in Proc. 9th Int. Workshop Inf. Security Appl., 2008, pp. 305–319.