RESEARCH ARTICLE OPEN ACCESS

PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System

S.Viji [1], E.DilipKumar[2]
[1]PG Student, [2]Associate Professor

[1, 2,] Department of MCA, Dhanalakshmi Srinivasan college of Engineering and Technology

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.

1. 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.

2. LITERATURE SURVEY

In this [1] we have outlined the importance and role of personal health management systems (PHMSs) along with some technical challenges and opportunities. In addition, there are a number of other challenges that need to be considered in order to enable PHMSs to achieve the expected level of operational dependability and establish their place in healthcare. The integration of PHMSs in healthcare implies their interconnection with health information systems (HISs) and electronic health records (EHRs). The most important requirement arising from this is the need for interoperability between PHMSs and HISs/EHRs. The potential of wearable and portable PHMSs to enable the shift to citizen-centered personalized care has been demonstrated through the work carried out under the European Commission's Fifth and Sixth Framework.

In this [2], we define the electronic healthcare record and present its purpose as a tool for continuity of care. We briefly describe the current situation of usage and focus on the major challenges to wide implementation in Europe and beyond. Finally, we point out trends that show stronger involvement of the patients-citizens in the health care prevention and promotion processes, and discuss the impact on the future development of the electronic healthcare record into personal health records.

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings.

Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

In this paper [4], we propose a new remote user authentication scheme using smart card. In our scheme, there are two attractive features: (i) no verification tables are required in the remote server; (ii) only one hash function computation and one modular multiplication computation are casted in smart card. Therefore, compared with other schemes, our scheme is more efficient.

Patient-controlled personal health record systems can help make health care safer, cheaper, and more convenient by facilitating patients to 1) grant any care provider access to their complete personal health records anytime from anywhere, 2) avoid repeated tests and 3) control their privacy transparently. In this paper [5], we present the architecture of our Privacy-aware Patient-controlled Personal Health Record (P3HR) system through which a patient can view her integrated health history, and share her health information transparently with others (e.g., healthcare providers). Access to the health information of a particular patient is completely controlled by that patient. We also carry out intuitive security and privacy analysis of the P3HR system architecture considering different types of security attacks. Finally, we describe a prototype implementation of the P3HR system that we developed reflecting the special view of Japanese society. The most important advantage of P3HR system over other existing systems is that most likely P3HR system provides complete privacy protection without losing data accuracy. Unlike traditional partially anonymous health records (e.g., using k-anonymity or l-diversity), the health records in P3HR are closer to complete anonymity, and yet preserve data accuracy. Our approach makes it very unlikely that patients could be identified by an attacker from their anonymous health records in the P3HR system.

In this paper [6] we present a series of protocols for authenticating an individual's membership in a group without revealing that individual's identity and without restricting how the membership of the group may be changed. In systems using these protocols a single message to the authenticator may be used by an individual to replace her lost key or by a trusted third party to add and remove members of the group. Applications in electronic commerce and communication can thus use these protocols to provide anonymous authentication while accommodating frequent changes in membership. We build these protocols on top of a new primitive: the verifiably common secret encoding. We show a construction for this primitive, the security of which is based on the existence of public-key cryptosystems capable of securely encoding multiple messages containing the same plaintext. Because the size of our construct grows linearly with the number of members in the group, we describe techniques for partitioning groups to improve performance.

3. 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. The disadvantages of the existing system is

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

4. PROPOSED SYSTEM

The main contributions of this paper are summarized as 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. The advantage of this is used to achieving data confidentiality and identity privacy with high efficiency.

5. MODULES

5.1 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.

5.2 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

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.

5.3 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.

5.4 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.

6. SCREEN SHOTS

The simulation result is present in the following:

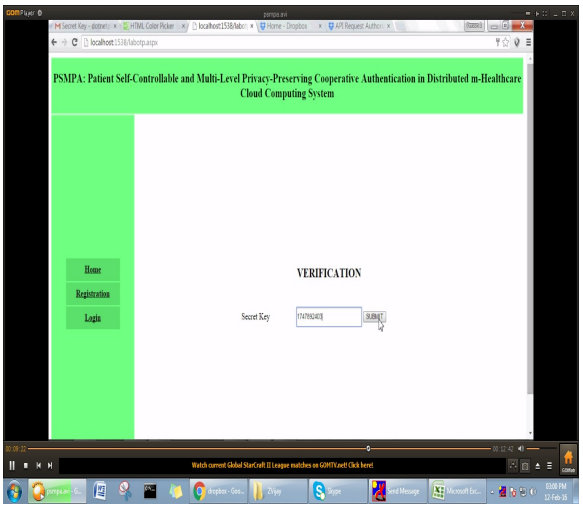

Fig 6.1 Enter the verification key received to lab mail

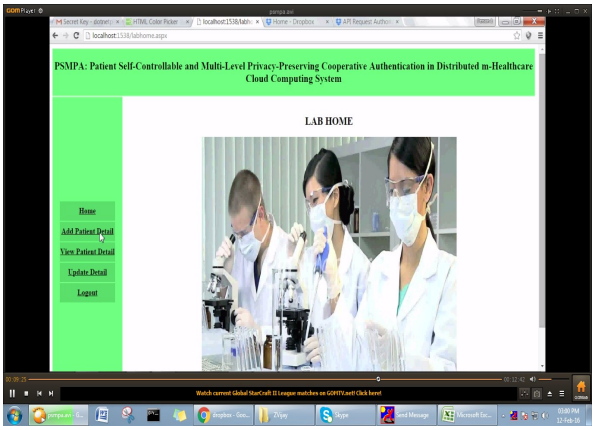

Fig 6.2 Add Details for existing patient in the lab

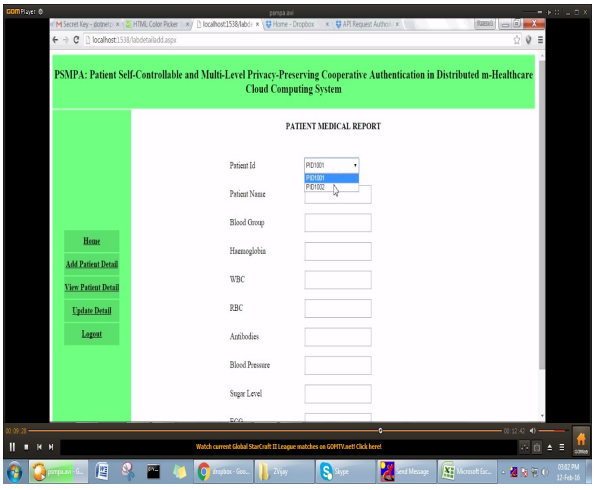

Fig 6.3 Enter the Patient ID

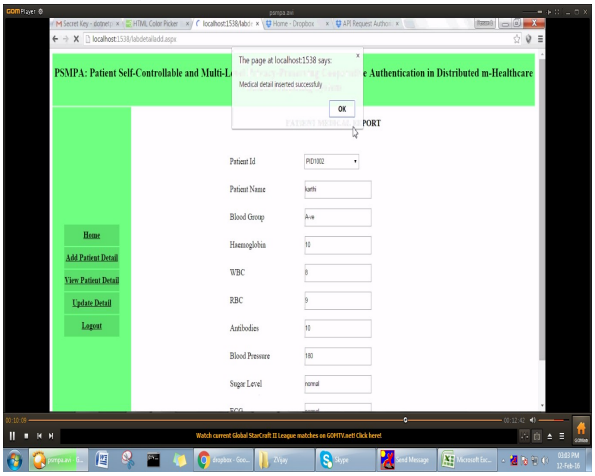

Fig 6.4 Enter all details and verified successfully

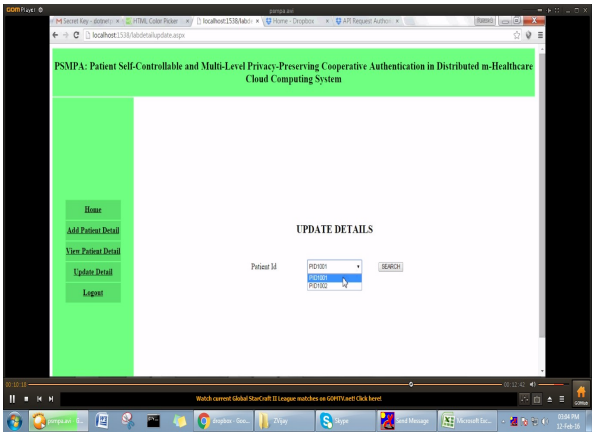

Fig 6.5 Update patient details in lab

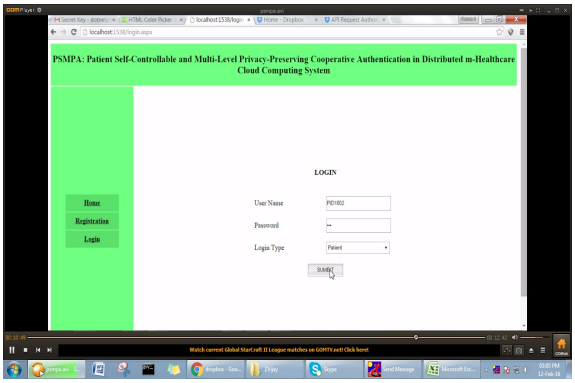

Fig 6.6 Lab person logout then Patient Login here

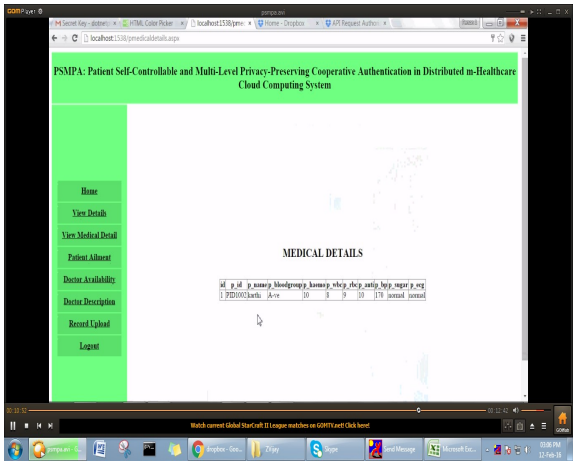

Fig 6.7 Verify the details added from library

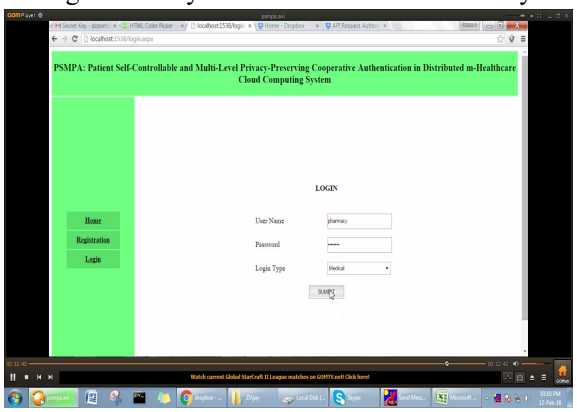

Fig 6.8 Pharmacy person Login here

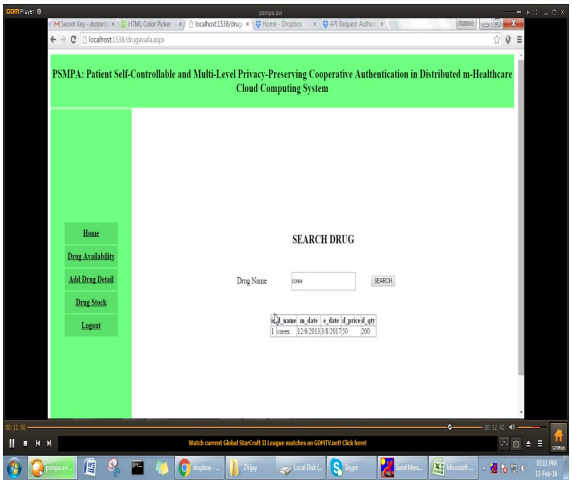

Fig 6.9 Search the drug

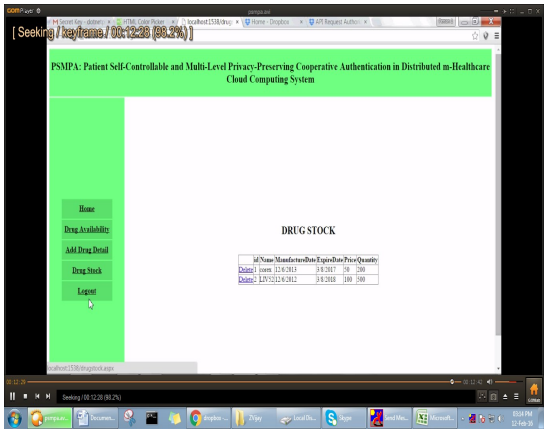

Fig 6.10 Show the drug stock then add or delete the drug details

7. CONCLUSION AND FUTURE WORK

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.

REFERENCES

1. L. Gatzoulis and I. Iakovidis, “Wearable and portable E-healthsystems,” 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 healthcarerecords 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 basedon 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 schemeusing smart card,” Comput. Netw., vol. 49, no. 4, pp. 535–540, 2005.
5. M. D. N. Huda, N. Sonehara, and S. Yamada, “A privacy managementarchitecture for patient-controlled personal healthrecord system,” J. Eng. Sci. Technol., vol. 4, no. 2, pp. 154–170,2009.
6. S. Schechter, T. Parnell, and A. Hartemink, “Anonymous authenticationof 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 mobilecomputing 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 secureand reliable data forwarding in vehicular delay tolerantnetworks,” in Proc. IEEE Global Commun. Conf., 2012, pp. 985–990.