Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.1 Issue 2 (2015) 13-17. Submitted 20/12/2015. Published 29/12/2015

A DISTRIBUTED M-HEALTH CARE CLOUD COMPUTNG SYSTEM WITH PATIENT SELF CONTROLLED AND MULTI LEVEL PRIVACY PRESERVING COOPERATIVE AUTHENTICATION

[1]K.Subasri, [2]C.Subasri, [3]B.Sholiya, [4]G.Sadiq Basha,
[1,2,3]UG Scholar, ECE Department, VRS College of Engineering and Technology, Villupuram,
[4]Associate Professor, VRS College of Engineering and Technology, Villupuram.

Abstract

Distributed m-healthcare systems significantly facilitate efficient patient treatment of high quality, while bringing about the challenge of keeping both the confidentiality of the personal health information and the patients' identity privacy simultaneously. It makes many existing data access control and anonymous authentication schemes inefficient in distributed m- healthcare systems. 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, a patient self-controllable privacy-preserving cooperative authentication scheme (PSCPA) realizing three levels of security and privacy requirement in distributed m-healthcare system is proposed. Many existing data access control and anonymous authentication schemes inefficient in distributed mhealthcare systems. To solve the problem, in this paper, establish a novel authorized accessible privacy model (AAPM) based on this propose a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA). Distributed m-healthcare realizing three levels of security and privacy requirement and patients can authorizes physicians by setting an access tree supporting flexible threshold predicates.

Key words – M-Health care, AAPM, PSCPA, PSMPA.

1. INTRODUCTION

In recent years, the distributed m-healthcare is emerged paradigm for exchanging the health information and allows to create, manage and control her personal health data, which has made the storage, retrieval, and sharing of medical information more efficient in cloud computing. The WHO defines the Mobile Healthcare is an area of the electronic health and it provide the heath information and services over mobile technologies such as mobile phones and personal digital Assistants (PDAs). The personal health information is always shared among the patients suffering from the same disease, between the patients and physicians as equivalent counterparts or even across distributed healthcare providers for medical consultant. This kind of personal health information sharing allows each collaborating healthcare provider to process it locally with higher efficiency and scalability, greatly enhances the treatment quality, significantly alleviates the complexity at the patient side and therefore becomes the preliminary component of a distributed m-healthcare system. As to the security facet, we mean the access control of 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 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. For example, the patients' insurance application may be rejected once the insurance company has the knowledge of the serious health condition of its consumers. Therefore, in distributed m-healthcare systems, which part of the patients' personal health information should be shared and which part of physicians should their personal health information be shared with have increasingly become two intractable problems

demanding urgent solutions. In this paper, simultaneously achieving both security and confidentiality with high efficacy. In distributed m-healthcare systems, all the members can be classified into three categories: the directly authorized physicians who are authorized by the patients, the indirectly authorized physicians who are authorized by the directly authorized physicians for medical consultant or research purpose and the unauthorized persons.

2. BACK GROUND

A. PHR CLASSIFICATION

PHRs can be classified based on the platform in which they can deliver the materials. There are two classifications: paper-based PHRs and Electronic PHRs. The below table shows the basic comparison between these two types:

PHR Class Property	Paper-based PHR	Electronic based PHR
Availability	Hardcopy	Softcopy
Accessibility	Locally	Globally
Protection	Open	Secure
Update	Difficult	Easy
Storability	On paper	On electronic carrier media
Distribution	Centralized	Distribution

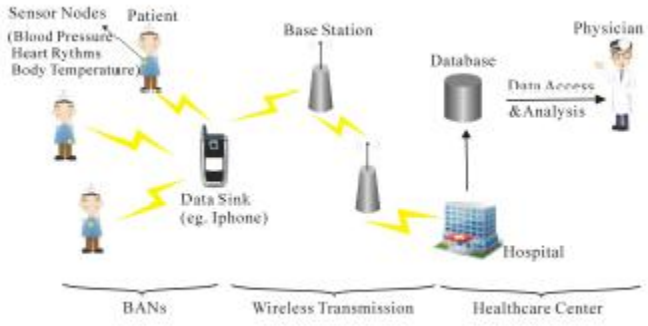
Table.1. The basic comparisons between Paper-based and Electronic-based PHR

In this paper, our proposed authorized accessible privacy model (AAPM) and the patient self-controllable privacy preserving authentication scheme (PSCPA) are proposed by extending the traditional designated verifier signature to an attribute based counterpart. The security and anonymity level is significantly enhanced by associating it to GBDH problem. Meanwhile, our construction cost is linear to the number of attributes rather than the physicians in healthcare providers. Therefore, it better adapts to the distributed m-healthcare systems where the number of physicians is great and the patients need the timely responses from the healthcare providers. Nowadays, most important to implement PHR models in healthcare management systems depends on the method of data entry, connectivity and availability. One of the popular models is standalone or free-standing PHRs which are often PC-based and require manual data entry to populate and up-date the record. These Standalone PHRs make the organization and storage of medical data very simple.

3. NETWORK MODEL

The most common free-standing PHRs are either paper-based, personal computer-based, or enabled by an Internet application. In general one can say that standalone PHRs provide basic tools that help people collect organize and store their health information. The basic e-healthcare system consists of three components: BANs, wireless transmission networks and the healthcare providers. Body sensor networks consist of various kinds of sensors monitoring and collecting all personal health information to the patient

hand-held mobile device. The wireless transmission networks transfer personal health information to the physicians in healthcare providers. The
healthcare provider consists of physicians and the patient information database (PIDs).



Fg.1. An Basic Architecture of the E-health System

Authorized physicians can access their corresponding patients' personal health information and authenticates their identities. The basic architecture of the E- healthcare system is illustrated in Fig. 1. Then, we further illustrate the unique characteristics of distributed m-healthcare systems where all the personal health information can be shared among patients, authorized physicians, distributed healthcare providers and medical research institutions.

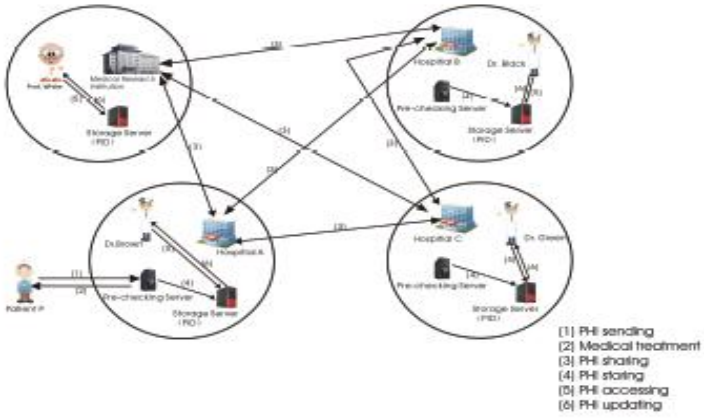


Fig.2. An Overview of Our Distributed m-Healthcare System

Then, we further illustrate the unique characteristics of distributed m-healthcare systems where all the personal health information can be shared among patients, authorized physicians, distributed healthcare providers and medical research institutions. A distributed m-healthcare system model is shown in Fig. 2.

4. ANALYSIS

The above mentioned schemes are not sufficient for efficiently processing the increasing the volume of personal health informational and also not enough for to only guarantee the data confidentiality of the patients personal health information in the honest-but-curious cloud server model since the frequently communication between a patient and a physician. Overcoming of this problem, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access

tree supporting flexible threshold predicates. a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare system is proposed. In Distributed Attribute-Based Encryption the focus is shifted from single trusted or central authority that knows the master key and circulates the secret attribute keys to the authorized users. In contrast there can be number of parties who can maintain attributes and their corresponding secret keys. This differs with the classic CP-ABE schemes, where all secret keys are distributed by one. A limitation of DABE requires a data owner to transmit an updated ciphertext component to every non-revoked user.

Techniques	Access control	Scalability	Efficiency	Flexibility	Security
ABE	High	High	Low	High	Low
KP-ABE	High	Low	Low	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	High	Low	Low	Low
DABE	Low	Low	High	Low	High

Fig.2. **comparisons of the schemes**

While sharing the information the communication overhead of key revocation is still high. The below table shows the comparisons of above mentioned algorithm with respect to access control, scalability, efficiency, flexibility and security. An identity-based encryption scheme, data is encrypted using an arbitrary string as the key and form decryption.

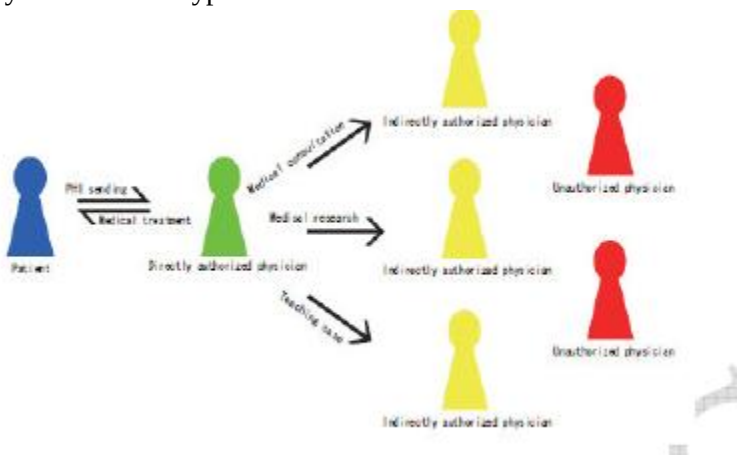


Fig.3. Multiple Security and Privacy Levels in m-Healthcare

A decryption key is mapped to the arbitrary encryption key by a key authority. There is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID

(PID) arbitrary strings. The directly authorized physicians are identified with green labels in the local healthcare provider they are authorized by the patients and these physicians can access the patient's personal health information and verify the patient's identity.

CONCLUSION

In this paper, a novel authorized accessible privacy model (AAPM) and a patient selfcontrollable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed mhealthcare cloud computing system are proposed and also avoided the some of the attacks occurred in the wireless communication medium.

REFERENCES

[1]. V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based Encryption for Finegrained Access Control of Encrypted Data, In ACM CCS'06, 2006.

[2]. M. Li, S. Yu, K. Ren and W. Lou, Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings, SecureComm 2010, LNICST 50, pp.89-106, 2010.

[3]. J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren, Attribute-based Signature and its Applications, In ASIACCS'10, 2010.

[4]. De-identified Health Information,
http://aspe.hhs.gov/admnsimp/bannerps.htm.

[5]. J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure HER System for Patient Privacy and Emergency Healthcare, ICDCS'11.

[6]. J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, Securing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions, IEEE Wireless Communications, vol. 20, No. 4, pp. 12-21, 2013