SECURING THE DATA CONFIDENTIALITY OF PATIENTS IN DISTRIBUTED M-HEALTHCARE CLOUD COMPUTING SYSTEM

Chandrika, Mahima.J, Yamuna.R, Swetha.P

[1,2,3] UG Student, [4]Assistant Professor Department of CS&E, RRCE, Visvesvaraya Technological University, INDIA.

Chandrika.cgowda@gmail.com, mahimajjayasimha@yahoo.com, yamunaranganath@gmail.com, shwetha6600@gmail.com

ABSRACT-Distributed m-healthcare computing system provides high quality patient treatment efficiently, but it brings number of challenges in safeguarding patients health information and identity privacy of patients. Many existing data access control and anonymous authentication systems are ineffective in distributed m-healthcare systems. To overcome this problem, in this paper, a authorized accessible privacy model (AAPM) is established. Distributed m-healthcare has three levels of security and privacy requirements and patients can authorize consultants by setting an access tree supporting flexible threshold predicates. Patients health information and personal information are verified by directly authorized, indirectly authorized and unauthorized physicians in medical consultation respectively satisfying the access tree with their own attributes.

Keywords- Access tree, distributed m-healthcare, privacy model, security, and threshold.

1. INTRODUCTION

1.1 Cloud Computing:

The cloud computing is based on internet computing that provides public processing resources and sources to computers and further devices on demand. It is a model for enabling universal on demand access to shared group of configurable computing resources. Cloud computation and storage solutions provide users and enterprises with various capabilities to store and process where data in third party Centre's. The cloud is a huge group of interconnected computers.

Computers can be personal computers or network servers; they may be public or private. Cloud of computers prolongs beyond a single company or enterprise. The application and data aided by the cloud are available to wide group of users, cross enterprise and cross stage. Access is via, the internet. Any authorized users can access these documents and applications from any computer over any internet connections. And to the users the technology and infrastructure behind the cloud is invisible. [1]

Cloud delivers a software platform that will enable customer to build an infrastructure-as-a service (Iaas) cloud. Cloud is built on the capabilities of existing virtualization management and physical servers provisioning solutions to deliver application to user that can be consumed in a self-service manner. Cloud optimizes the usage of physical and virtual organization through intelligent resource. Allocation policies and add the ability to flex applications elastically based on the demand.

1.2. m-healthcare:

M-healthcare is an abbreviation for mobile healthcare, a word used for the practice of medicines and public health records maintained by mobile devices. The term is most commonly used in reference to using communication devices like mobile phones, PDAs and tablet computers for health facilities and information, but also to affect emotional states. This paper contains Distributed m-healthcare cloud computing system provides high quality patient treatment for medical consultation by sharing patient's personal health information among hospitals. It brings series of challenges mainly how to ensure the protection and confidentiality of the patient's personal information and health information from the different type of attacks in the wireless communication channel. One of the main challenges is access control of patient personal health information. Access control is the policy driven limitation of access to system data and dialogs. Access permission defines whether a role or individual should have any access to all and, if so, exactly what the role or individual should be allowed to do the resource.[3]. Namely it is only the physicians or consultancies that have privilege to access the data that can recover the patient's personal health information during data sharing in distributed m-healthcare computing system.

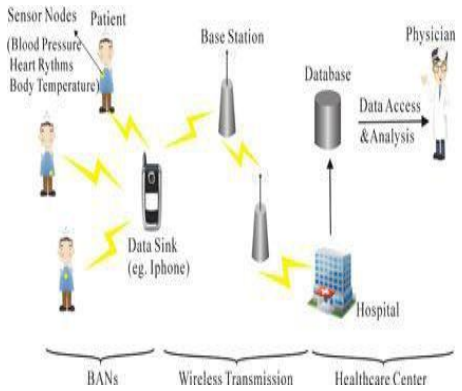

Fig. 1 The Architecture for the m-healthcare system.

The basic m-healthcare system illustrated in Fig.1 mainly consists of three components: body area networks (BANs), wireless networks and the healthcare organizations furnished with their own cloud servers [1], [2]. The patient's personal health information is securely sent to the healthcare provider for the physicians to access and perform medical treatment. We further illuminate the unique characteristics of distributed m-healthcare cloud computing systems where all

the personal health information can be shared between patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare organizations and medical research institutions for medical consultation.

2. WORKING METHODOLOGY

In m-healthcare social networks, the information about the person‘s health and his/her personal information are always shared between 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.As to the security aspect, one of the main issues is access control of patients‘ personal health information, namely it is only the physicians or institutions that can recover the patients‘ personal health information during the data sharing in the distributed m-healthcare computing system.A fine-grained distributed data access control scheme is suggested using the technique of attribute based encryption (ABE). A rendezvous-based access control scheme provides access privilege if and only if the patient and the physician meet in the physical world. Now a days, a patient-centric and fine-grained data access control in multi-owner settings is constructed for safeguarding personal health data in cloud computing. However, it mainly focuses on the central cloud computing system which is not enough for efficiently processing the increasing volume of personal health information in m-healthcare computing system. Furthermore, it is not enough for to only promise the data confidentiality of the patient‘s health information in the cloud server model since the frequent communication between a patient and a physician can lead the opponent to conclude that the patient is suffering from a particular disease with a high possibility. Unfortunately, the problem of how to secure both the patients‘ data confidentiality and identity privacy in the distributed m-healthcare computing scenario under the malicious model was left untouched.To overcome this disdvantages, we propose a novel authorized accessible privacy model for distributed m-healthcare cloud computing system.

2.1. Authorized accessible Privacy Model (AAPM)

Several existing access control and anonymous authentication systems cannot be clearly exploited. To overcome the problem, in this paper, we established a novel that is authorized accessible privacy model(AAPM). Patients can authorize physicians by setting an access hierarchy supporting flexible threshold establishes to access their information provided to the hospital database. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable privacy-preserving authentication scheme realizing three levels of security and privacy requirement in m-healthcare computing system is proposed. The directly authorized physicians, the physicians who are indirectly authorized and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or validate patients‘ identities by satisfying the access tree with their own attribute sets.

Lastly, the security proof and simulation results illustrate our scheme can resist different kinds of attacks and far outperforms the prior ones in terms of computational, communication and storage overhead. A basic architecture of a distributed m-healthcare cloud computing system is shown in Fig. 3

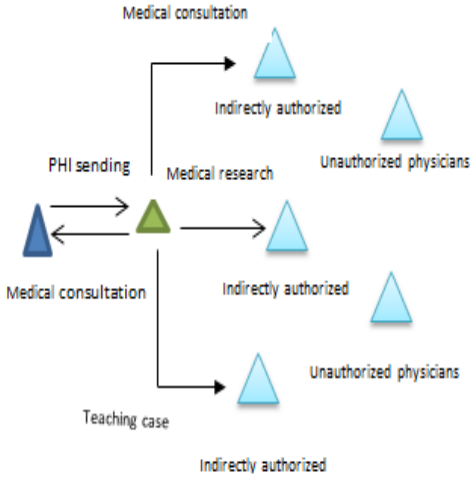

Fig. 2. Security and privacy levels in m-healthcare computing system.

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

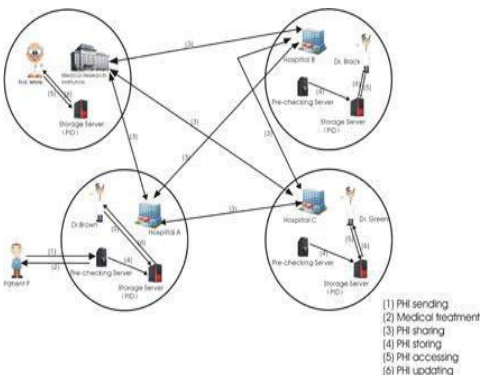

Fig. 3.An overview of m -healthcare cloud computing system.

Table.1 Access control on patient's data

Data	Directly authorized physicians	Indirectly authorized physicians	Unauthorized physicians
Personal Information	**YES**	**NO**	**NO**
Health Information	**YES**	**YES**	**NO**

3. CONCLUSION

In this paper, authorized accessible privacy model (AAPM) ,a novel is established and a patient self-controllable privacy-preserving authentication scheme realizing three levels of security and privacy requirement in the distributed m-healthcare system are proposed, followed by the formal security evidence and efficiency evaluations. Patients can provide privileges to the physicians by setting an access tree supporting flexible threshold predicates. The directly authorized doctors, the indirectly authorized doctors and the unauthorized physicians would know both personal data of patient's and the health information of patients, only the personal health information and nothing respectively. Finally, simulation results show our project far performs prior schemes in terms of storage, computational and communication overhead.

4. ACKNOLEDGEMENT

The author would like to thank Karnataka State Council for Science and Technology(KSCST) for funding this proposal (with serial number 39S_BE_1029). This work is carried out at project laboratory, department of computer science and engineering, RajaRajeswari College of Engineering

REFERENCES

[1]. Michael Miller ―*Cloud Computing*‖, Pearson Education, Inc, 2013.
[2]. Dr Kumar Saurabh ―*Cloud Computing*‖ Wiley pvt, second edition,2013.
[3]. Raymond R. Ranko ―*Corporate computer and Network Security*‖, pearson Education, Inc, 2003
[4]. V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based Encryption for Finegrained Access Control of Encrypted Data, In ACM CCS'06, 2006.
[5]. 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.
[6]. J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren, Attribute-based Signature and its Applications, In ASIACCS'10, 2010.
[7]. De-identified Health Information, http://aspe.hhs.gov/admnsimp/bannerps.htm.
[8]. J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography Based Secure HER System for Patient Privacy and Emergency Healthcare, ICDCS'11.
[9]. 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