ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Secure Data Sharing Health Data in Different Cloud Server

Same Naik Kondlavath
PG Scholar
Department of CSE
SVR Engineering College,
Ayyaluru, Nandyal.

K.Amarendhranath
Assistant Professor
Department of CSE
SVR Engineering College,
Ayyaluru, Nandyal.

ABSTRACT

Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. Patient self-controllable privacy-preserving cooperative authentication scheme realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. Database has been considered to be very important since a really long time and securing it now is of utmost importance-healthcare systems is very popular now but faces security constraints. The distributed m-healthcare systems allow significant patient treatment for medical consultation by sharing personal health information among healthcare providers. The important challenge is to ensure the security of the patient's identity as well as the data. Patients can decide which physician can access their information by using threshold predicates. Based on this idea we are devising a new technique where the patient can self-control their data with different ways of security. The directly authorized physicians and the patient can respectively decipher the personal health information and/or verify and update patient's health information at the click of a button

Keywords: - ***Security Authentication Access Control; Distributed Cloud Computing; M-Healthcare System; Security and Privacy.***

INTRODUCTION

Distributed m-healthcare cloud computing systems have been increasingly adopted 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 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 has 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.

RELATED WORK

Existing System

A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). A rendezvous-based access control

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.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. 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 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.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.

Proposed system

In this paper, we consider simultaneously achieving data confidentiality and identity privacy with high efficiency. 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.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.

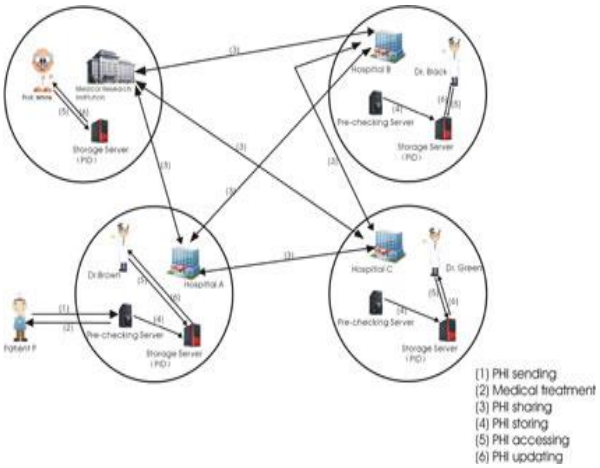

Fig:-1 an Overview of Distributed m-Healthcare Cloud Computing System

IMPLEMENTATION

Directly authorized physicians:

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Indirectly authorized physicians:

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.

M-Healthcare Cloud Computing:

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.

EXPERIMENTAL RESULTS

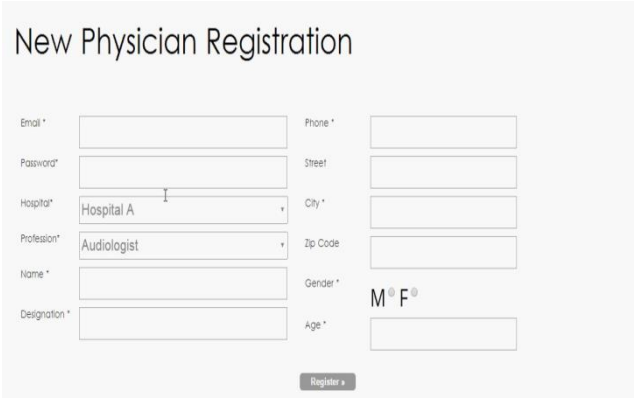

Fig:-2 Registration Page

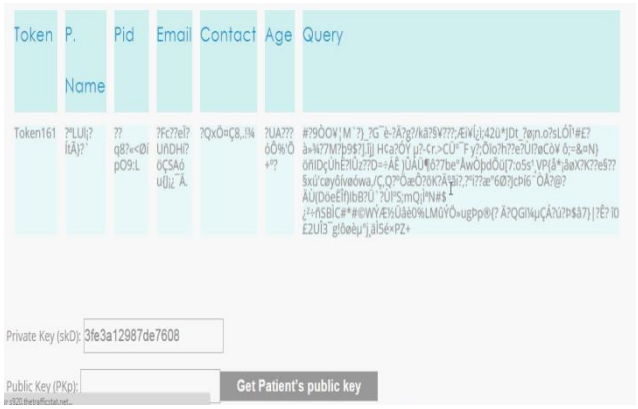

Fig:-3 Data Encryption

Fig:-3 Data Request

Fig:-4 Key generation

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION

In this paper, a new authorized available solitude model and a patient self-controllable multi-level solitude preserving helpful verification scheme apprehending three dissimilar levels of safety and solitude obligation in the dispersed m-healthcare cloud computing method are planned, pursued by the official safety proof and competence assessments which exemplify our PSMPA can oppose different sorts of malicious assails and far outperforms preceding schemes in terms of storage, computational and communiqué 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.

[9] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributeddata 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 controlfor medical records in the pre-hospital environment," in Proc. 1st ACM SIGMOBILE Int. Workshop Syst. Netw. Support HealthcareAssisted Living, 2007, pp. 1–6.