Volume 3, Issue 8, August-2016, pp. 436-440 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

A Multi-level Self-Controllable Authentication in Distributed m-Healthcare Cloud Environments

A.Yogananda[1] and Chepuri Sai Teja[2]

[1] Assistant Professor, Dept of CSE, MRCET, Hyderabad, Telangana.

[2] Pursuing M.Tech, Dept of CSE , MRCET, Hyderabad, Telangana.

Abstract :-Secrecy in the distributed m-healthcare cloud computing reflect concurrently attaining data confidentiality and identity privacy with high efficiency in this connection Cloud Computing providing several advantages to service providers and to customers, Hence it have a good preference in the technical world. The health care industries are growing in various fields over the few years. For the patients and doctors or to other physicians the communication is an important requirement for the inquiries and suggestions. The m-Healthcare cloud computing is significantly providing such type of communication for efficient patient treatment and medical consultation by sharing the personal health information to health care service providers (Hospitals, Research Centres etc.). Even though a service is good there are some privacy breaches in the present scenario they are following. They are (1) Data Confidentiality and (2) Patient's Identity Privacy. Much existing access and authentication schemes introduced by several types of research but they cannot be exploited in a straightforward manner. To solve this issue, in this paper we propose an Authorized Accessible Privacy Model (AAPM). By this, a patient can authorize a physician by setting a multi-level access tree of threshold predicates. According to this, we introduce a new technique called attribute-based designated verifier signature for multi-level patient self-controllable authentication in cloud computing environment realizing three levels of privacy and security requirement in distributed m-Healthcare cloud computing system. The three levels of authentication involve directly authorized a physician, indirectly authorized physician and unauthorized persons for medical consultation and decipher the personal health information and to verify the identities by satisfying the access with the help of their own set of attributes.

Key Words: Cloud Computing, Distributed m-Healthcare, Authorized Accessible Privacy Model, Data Confidentiality

1. INTRODUCTION

Organizations are increasingly becoming dependent on the Internet for sharing and Accessing information. This Internet boom has changed the focus of application development from stand-alone applications to distributed Web applications. The Distributed m-healthcare systems have been highly adopted by European Commission of activities, foreign and US Health Insurance Portability and Accountability Act and many governments for the efficient and high-quality treatment. In this paper, we tend to consider at the same time achieving data confidentiality and identity privacy with high efficiency. As is delineate in Fig. 1, in the distributed m-health care cloud computing systems, all the members may be classified into three categories: the directly approved physicians with green labels in the local healthcare provider who are approved by the patients and may both access the patient's personal health data and verify the patient's identity and also the indirectly approved physicians with yellow labels within the remote health care providers who are approved by the directly approved physicians for a medical authorities and some analysis functions (i.e., since they're not approved by the patients, we tend to use the term 'indirectly authorized' instead). They'll solely access the private health info, but not the patient's identity information. For unauthorized persons with red labels, nothing might be gained. By extending the techniques of

 DOI: 05.2016-75251336/IJCERT.2016.3810

attribute based mostly access management and designated verifier signatures (DVS) on de-identified health data, we tend to understand three totally different levels of privacy-preserving demand mentioned above.

A personal health data is often shared among the patients affected by an equivalent disease, between the patients and the physicians as the equivalent counterparts or maybe across distributed health care providers for medical authority. this type of non-public health info sharing permits every collaborating health care provider to process it regionally with higher potency and quantifiability, greatly enhances the treatment quality, considerably alleviates the complexness at the patient aspect and so becomes the preliminary element of a distributed m-healthcare system. However, it additionally brings a couple of series of challenges, particularly a way to make sure the security and privacy of the patients' personal health info from numerous attacks within the wireless communicating resembling eavesdropping and meddling.

As to the protection aspect, we tend to mean the access management of private health data; particularly it is only the approved physicians or establishments that may recover the patients' personal health info throughout the information sharing within the distributed m-healthcare system. In following, most patients are involved regarding the confidentiality of their personal health info since it's doubtless to create them in bother for every kind of unauthorized assortment and disclosure. Let's say, the patients' insurance application is also rejected once the insurance firm has the information of the intense health condition of its customers. Therefore, in distributed m-healthcare systems, which a part of} the patients' personal health info ought to be shared and that part of physicians ought to access their personal health data be shared with have progressively become two intractable issues demanding imperative solutions. There has emerged numerous analysis that specializes in it resembling a fine-grained distributed data access management scheme exploitation the technique of attribute based mostly encryption and a rendezvous-based access management methodology providing access if and provided that the patient and also the physician meet within the physical world. Unfortunately, the matter of simultaneously protective patients' privacy was left unresolved.

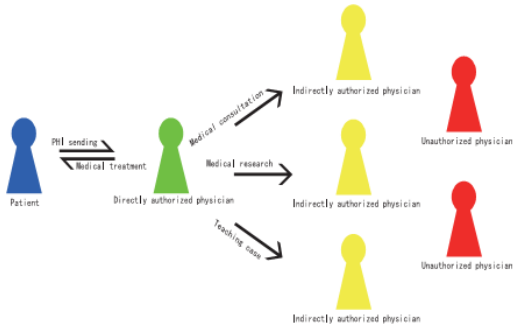


Fig.1. Security and Privacy levels in m-Healthcare cloud computing

In this paper, we tend to contemplate simultaneously achieving information confidentiality and identity privacy with high potency. As is delineated in Fig. 1, in distributed m-healthcare cloud computing systems, all the members is classified into three categories: the directly licensed physicians with green labels in the local care supplier who are approved by the patients and may each access the patient's personal health data and verify the patient's identity and also the indirectly licensed physicians with yellow labels within the remote care providers who are approved by the directly approved physicians for medical authority or some analysis functions (i.e., since they're not approved by the patients, we tend to use the term 'indirectly authorized' instead). they will only access the private health data, but not the patient's identity. For all the unauthorized persons with red labels, nothing might be obtained. By extending the techniques of attribute primarily based access management and designated verification signatures (DVS) on de-identified health data, we tend to understand three various levels of privacy-preserving demand mentioned above.

2. PRESENTED SYSTEM

Distributed healthcare system notably warrants efficient patient treatment for medical examination by sharing personal health information among medical care services. Physicians it induces the challenge of keeping together the data confidentiality and patient's identity privacy altogether. To a large extent existing access control and anonymous authentication schemes cannot be without difficulty exploited. M-healthcare social

 DOI: 05.2016-75251336/IJCERT.2016.3810

networks the personal health details are always shared among the patients present in specific social societies afflicted by the same disease for common support and across distributed healthcare providers own cloud servers for the medical professional. The security and safety of the patients' personal health information from various attacks in the wireless network channel. Considered one of the main issues is access control of patients' personal health information particularly it is only the approved physicians or institutions that can recuperate the patients' personal health information during the data sharing in the distributed m-healthcare cloud computing system.In this article, a security and safety and anonymity higher standard of our proposed development might be more substantially transformed by partnering it with the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and a number of patients' characteristics to process secrecy seepage inpatient sparsely distributed environment. More noticeably, without a knowledge of which physician in a healthcare provider is professional in treating his illness and complication, the most effective way for the patient could be encrypted his own PHI (personal health information) under a certain access policy in lieu of assign each physician a secret key. Consequently, the authorized physicians whose attribute set fulfill access policy can extort the PHI and access control management also becomes more conveniently.

Fig.2. A basic e-healthcare system

3. FRAMEWORK

A. Network Model

The basic e-health care system described in Fig. 2 mainly consists of three components: body area networks, wireless transmission networks and health care service providers equipped with their own cloud servers. The patient's personal health information is securely transmitted to the health care provider for the authorized physicians to access and perform the medical treatment.

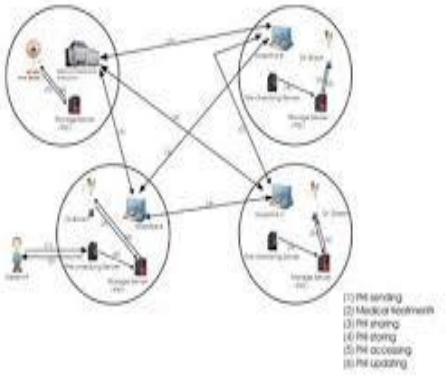


Fig.3. m-Healthcare cloud computing system.

The architecture of a distributed m-health care cloud computing system has been shown in Fig. 3. There are three distributed healthcare providers K ; L ; M and a medical research center N, where the doctors and Prof are working respectively in this. Each one of them possesses their own cloud server. It is assumed that the patient P registers at hospital A, all her/his health information are stored in the hospital.

A's cloud server, and doctors are one of his directly authorized physicians. For the medical consultation or the other research purposes in cooperation with hospitals L and M and medical research centre N, it is needed for doctors to generate the three indistinguishable transcript simulations of the patient P's health information and to share them among the distributed cloud servers of hospitals L and M and medical research centre N.

B. Authorized Accessible Privacy Model

In this aspect, we advise a new validated accessible privacy platform for a distributed m-health care cloud computing systems which possesses the specified two components: attribute based stipulated verifier signature scheme (ADVS) and associated adversary model of a system.

Attribute based Designated Verifier Signature Scheme:

We propose to her a patient self-controllable and multi-level privacy-preserving accommodating authentication format as per ADVS to construct

 DOI: 05.2016-75251336/IJCERT.2016.3810

three levels of security and privacy applications in the distributed m-health care cloud computing which in effect possess the following five algorithms: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation. Which denotes the universe of attributes as U. We say an attribute set v satisfies a specific access structure A if and if $A(\omega) = 1$ where ω is chosen from U. The algorithms are defined as follows.

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

Key Extract: Suppose a physician requests an attribute set $\omega_D \in U$. The attribute authority computes sk_D for him if he is eligible to be issued with sk_D for these attributes.

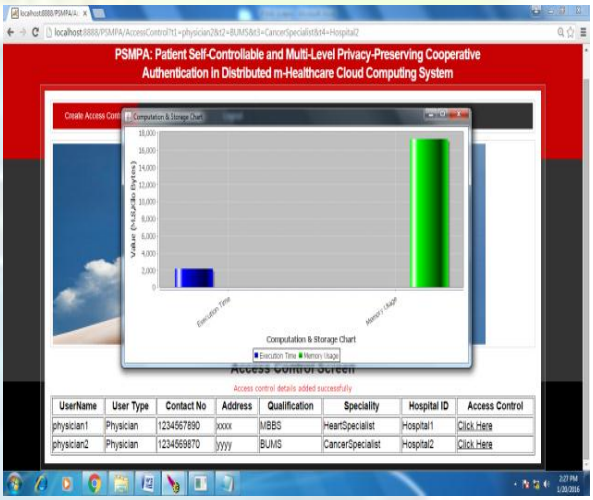
Sign: A deterministic algorithm that uses the patient's private key sk_p, the uniform public key pk_D of the healthcare provider where the physicians work and a message m to generate a signature σ. That is, $\sigma \leftarrow Sign(sk_p, pk_D, m)$.

Verify: Assume a physician wants to verify a signature σ with an access structure A and possesses a subset of attributes $\omega_j subset\ of\ \omega_D$ satisfying A(ω_j) = 1, a deterministic verification algorithm can be operated. Upon obtaining a signature σ, he takes as input his attribute private key sk_D and the patient's public key pk_p, then returns the message m and True if the signature is correct, or ⊥ otherwise. That is, {True, ⊥} ← Verify(sk_D, pk_p, m, σ).

Transcript Simulation Generation: We have a requirement that the directly authorized physicians who have the authorized secret/private key skD can always produce the identically distributed transcripts nondistinguishable from the original protocol through the Transcript Simulation algorithm. Due to the fact that a Transcript Simulation algorithm can generate the identically distributed transcripts indistinguishable from original signatures, hence the patient's identity can be well protected from the indirectly authorized physicians for persons for whom only the transcripts are delivered.

4. EXPERIMENTAL RESULTS

In cloud computing in previous, there are several types of research which have given the appropriate solution for m-healthcare service. They have concentrated on the data confidentiality rather than user or patient by a centralized architecture. In this paper, we have introduced a novel authorized accessible privacy model privacy and security. We consider simultaneously achieving the data confidentiality and the identity privacy with high efficiency. Hence the experimental result shows that the given approach satisfies the requirements of a system.



5. CONCLUSION

In this paper, an approved patient self-controllable multi-level privacy and authentication process of distinct degrees of security and safety and privacy specification in the healthcare system are proposed, followed by the traditional security evidence of and effective critical reviews which express our PSMPA can combat various kinds of serious attacks and far outperforms earlier schemes with respect to the storage, computational and the communication costs.

REFERENCES

[1] L. Gatzoulis and I. Iakovidis, "Wearable and portable E-health systems," I EE E E n g . Me d . B I o l . M a g., vol. 26, no. 5, pp. 51–56, Sep.-Oct. 2007.

 DOI: 05.2016-75251336/IJCERT.2016.3810

[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] 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.

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

[5] 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.

[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] 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.

[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] 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.

 DOI: 05.2016-75251336/IJCERT.2016.3810