International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 –APRIL 2016.

Patient Self-Controllable and Authorized Accessible Privacy Model in Distributed m-healthcare Cloud Computing System

Narmatha. P[1], Dharani Manoharan.B[2]
[1]PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu-624619, India.
[2]Assistant Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu-624619, India.

Abstract-Distributed m-healthcare systems provide an impeccable treatment for patients. The decisions were made of high quality. Yet, it provides a series of challenges in personal health information. Previous works are incapable of producing efficient distributed m-healthcare systems. In this paper, we presented novel Authorized Accessible Privacy Model (AAPM) that depicts patient's self-controllable systems through multi-level Privacy preserving Cooperative Authentication Scheme). The proposed method activates the security and privacy requirements of the patients. Experimental designs demonstrated the effectiveness of the system.

Keywords: Distributed system, Personal information, Privacy model, Authorization and Cooperation Scheme.

I INTRODUCTION

Distributed m-healthcarecloud computing idea has beenraised lately. We can say that it is a patient driven model as general control of patient's information is with patient. Because of the high cost of building and keeping up the data centers, a third party administration suppliers give health administration. Be that as it may, while utilizing third partyservices, there are numerous security and protection dangers in the framework. In m-healthcare interpersonal organizations, the individual data is constantly shared among the patients situated in particular social groups experiencing the same ailment for common support, and crosswise over conveyed human services suppliers furnished with their own cloud servers for medicinal specialist in disseminated m-medicinal services distributed computing frameworks.

As of late, the dispersed m-healthcare is novel frameworks for trading the wellbeing data and permits to make, oversee and control her information by themselves, which has made the capacity, recovery, and sharing of restorative data to more productive in cloud computing. The WHO characterizes the Mobile Healthcare is a region of the electronic wellbeing and it give the heath data and administrations over portable advances, for example, cellular telephones or also, Personal Digital Assistants (PDAs).The individual wellbeing data is constantly shared among the patients enduring from the same sickness, between the patients and doctors as comparable partners or even crosswise over circulated social insurance suppliers for restorative specialist. This sort of individual wellbeing data sharing permits each working together human services supplier to process it locally with higher productivity and adaptability, enormously upgrades the treatment quality, fundamentally eases the multifaceted nature at the patient side and in this manner turns into the preliminary part of a distributed m-healthcare systems. In conveyed m-healthcare distributed computing framework, as it were the approved doctors or a foundation that can recuperate the patient's data amid information sharing. Most patients are worried about the privacy of their personal health data since it is liable to make them in inconvenience for every sort of unapproved accumulation and revelation.

Therefore, in distributed healthcare a system, which part of the patients' personal health information should be shared and which part of physicians should their personal health information be sharing is the main problem. Here, simultaneously achieving both security and confidentiality with high efficiency. 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.

The paper is organized as follows: Section I describes the basic definitions of m-healthcare information systems. Section II describes the related work studied in m-healthcare systems. Section III describes the proposed work.

Section IV describes the experimental designs of the systems. At last, concluded in Section V.

II. RELATED WORK

A Cryptographic Key Management Solution (CKMS) for HIPAA Privacy/Security Regulations was proposed by B. Lee and C.D Lee (2008) in which the security regulations stipulate the procurements to protect information respectability, privacy, also, accessibility and less significance is given to tampering.

A configuration for a protected interoperable cloud-based Individual Health Record administration was proposed by Hsieh, G. et al, (2012). In this paper, the portability and interoperability was improved utilizing the Congruity of Care Document (CCD).This was utilized for both putting away and trading the PHR data for a person.

Security and crisis reaction in e-healthcare utilizing remote body sensor systems proposed by Jinyuan Sun et al, (2010) a model for utilizing Wireless Body Sensor Networks (WBSN) which requires that some Body Sensor gadgets should be connected to the patient dependably. The constrained accessibility of the body sensors, the procedure gets to be repetitive. The area security of the patients gets to be an inquiry since the patient's body sensors are persistently followed, the area about the patient likewise gets overhauled which is a genuine security and security issue.

Cryptography Based Secure EHR System for Quiet Privacy and Emergency Healthcare was proposed by Jinyuan Sun et al, (2011), which gives sufficient protection to the patients utilizing progressed cryptographic instruments furthermore gives a choice for giving treatment to the patients on the off chance that of a crisis purposes. It meets the security objectives, for example, the privacy, accessibility, access control, information respectability and neglects to support the eavesdropping and tampering.

A secure m-healthcare social networks with its challenges, counter measures and future directions was proposed by Jun Zhou, et al (2013). A wide range of cyber-attacks are inculcated into this paper. It also provides the distributed architecture of the mhealthcare system. In this design, each of the node chooses an optimal link which possesses the highest predicted quality. Authorized Private Keyword Search over Encrypted Personal Health Records was proposed by Li, Ming et al, (2011), a scheme which brings in the necessity of search. It also deals with the authorization which reduces the privacy exposure from the search results. It establishes a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data.

A novel solutions dealing with the technicality for the purpose of maintaining the privacy of EHR was proposed by P. Ray et al (2006). Since the information that are present in this records contains patient healthcare information that needs to be shared amongst the healthcare providers and professionals. The privacy of the EHR have been an impediment to the implementation of the EHR/ EPR /EMR systems. Spoc: It is a secure and an opportunistic computing framework in case of an emergency in mobile healthcare was proposed by R. Lu et al, (2013). It is based on a scalar product computation technique which is extensively used for privacy preserving, since each and every attribute requires a scalar product calculation it meets with computation overhead in processing the PHI data. The Security Models and Requirements for the Healthcare Application in Clouds was proposed by R. Zhang, et al (2010). It describes a security reference model in the arena of EHR for the sake of managing the security issues. It highlights three important components in securing an EHR cloud. They are the, countermeasure, state of art techniques and the use case scenario.

Physiological Signal based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems was proposed by S.-D. Bao, et al (2005) in which a unique solution is provided in order to handle the entity authentication in body area sensor network is provided. Exploiting Prediction to Enable Secure and Reliable Routing in Wireless Body Area Networks was proposed by X. Liang, et al (2012). This paper provides a Prediction based Reliable routing framework for emerging Wireless Body Area Networks. It can be unified with a specific routing protocol. SAGE: A Strong Privacy-Preserving Scheme against Global Eavesdropping for ehealth Systems was proposed by Xiaodong Lin et al, (2009). This was a scheme developed against eavesdropping for the ehealth systems. Since the main focus of the paper is on eavesdropping, the other types of security breaches such as tampering were not much taken into consideration. Security and privacy in RFID and its applications was proposed by Y. Xiao, et al (2006) in telemedicine is provided. Radio frequency identification systems provide many interesting applications which help in telemedicine, inventory control and supply chain management.

III. IMPROVISED m- HEALTHCARE SYSTEMS

The improvised m-healthcare system is executed in four ways:

a) System Model
b) Signature Scheme
c) PSPMA design
d) Anonymity for the patient

a) System Model

In the primary module, we build up the fundamental e-health services framework which comprises of three parts: Body Area Networks (BANs), remote transmission systems and the medicinal services suppliers furnished with their own particular cloud servers. The patient's personal health data is safely transmitted to the services supplier for the approved doctors to access and perform restorative treatment. Then we further outline the novel attributes of conveyed m-health services distributed computing frameworks where all the human data can be shared among patients experiencing the same infection for common support or among the approved doctors in disseminated medicinal services suppliers and restorative exploration foundations for the therapeutic process.

b) Signature Scheme

We propose a patient self-controllable and multi-level protection plan in light of ADVS to acknowledge three levels of security and privacy necessity in conveyed m-health cloud computing framework which for the most part comprises of the accompanying five estimations: Setup, Key Extraction, Sign, Verify and Transcript Simulation Generation. In anattribute based assigned verifier signature plan, as to unforgeability, we imply that the enemy needs to fashion a signature w.r.t an unsatisfied verifier's particular access structure. The meaning of unforgeability permits an enemy not to create a compelling signature with an entrance structure.

c) PSMPA Design

In this module, we give an outline of the proposed PSMPA to actualize AAPM presented beforehand, acknowledging three distinct levels of security and protection prerequisites. The signing calculation yields a signature of the patient's personal data m which must be recouped and confirmed by the straightforwardly approved doctors whose arrangements of properties fulfill the access tree. In our proposed PSMPA, for specifically approved doctors, performing the Verify calculation permits them to both translate the patient's character utilizing the private key of the patient's enlisted nearby social insurance supplier and recoup the patient's personal information m utilizing the approved characteristic private key. In this way, the unlinkability between the patient character and his own data can be protected.

d) Anonymity for the patient

To ensure a solid protection for the patient, the signature uncovers nothing about the personality of the patient with the exception of the data unequivocally uncovered. For unapproved persons (enemies), nothing could be acquired. It is likewise watched that for the last two classes, distinctive marks created by the same patient can't be linkable without knowing his real personality.

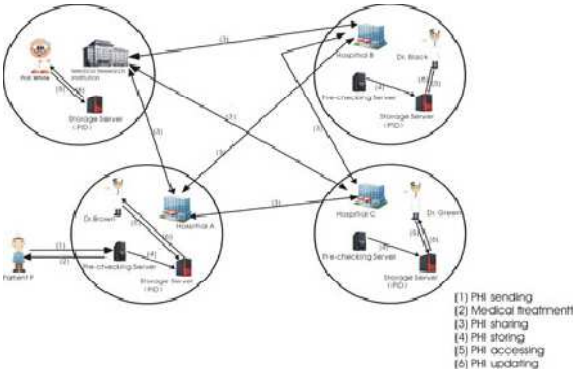

Fig.1. System Architecture

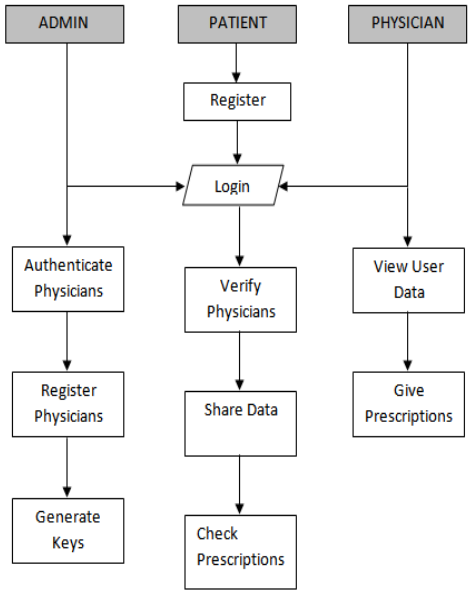

Fig.2. Proposed Architecture

V. CONCLUSION

The enhanced multilevel privacy preserving m-health cloud computing system increases the security and privacy of the patients' personal health records from different types of attacks such as eavesdropping and tampering. In this paper, we have proposed an enhanced multilevel m-healthcare system, in which we have enhanced the existing techniques like a novel Authorized Accessible Privacy Model (AAPM) and attribute-based designated verifier signature. In this method the security is increased since the patient's attributes are encrypted using password based encryption, and also encrypted using hash function of the salt and attribute together using the SGHG algorithm and

also it deals with the privacy leakage. The security and anonymity level of our proposed construction is enhanced in multilevel privacy preserving m-healthcare system.

REFERENCES

[1] Lee, B. and C.-D. Lee, 2008 “A cryptographic key management solution for HIPAA privacy/security regulations,” IEEE Trans. Information Technology in Biomedicine, 12(1): 34- 41.

[2] Hsieh, G., R.-J. Chen, 2012. Design for a secure interoperable cloud-based Personal Health Record service, Cloud Computing Technology and Science (CloudCom), pp: 472-479.

[3] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang; Yuguang Fang, 2011. HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare, Distributed Computing Systems (ICDCS), pp: 373-382.

[4] Jinyuan Sun; Yuguang Fang; Xiaoyan Zhu, 2010. Privacy and emergency response in ehealthcare leveraging wireless body sensor networks, Wireless Communications, 17(1): 66-73.

[5] Jun Zhou; Zhenfu Cao; Xiaolei Dong; Xiaodong Lin; A.V. Vasilakos, 2013. Securing m-healthcare social networks: challenges, counter measures and future directions, Wireless Communications, 20(4): 12-21.

[6] Li, Ming; Shucheng Yu; Ning Cao; Wenjing Lou, 2011. Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing, Distributed Computing Systems (ICDCS), pp: 383- 392.

[7] Ray, P. and J. Wimalasiri, 2006 “The need for technical solutions for maintaining the privacy of EHR,” in Proc. 28th IEEE EMBS Annual International Conference, pp: 4686-4689.

[8] Zhang, R. and L. Liu, 2010, "Security Models and Requirements for Healthcare Application Clouds," Proc. 2010 IEEE 3rd Int'l Conf. on Cloud Computing, pp: 268-275.

[9] Bao, S.-D., Y.-T. Zhang and L.-F. Shen, 2005. “Physiological Signal based Entity Authentication for Body Area Sen-sor Networks and Mobile Healthcare Systems,” Proc. 28th IEEE EMBC, pp: 2455-2458.

[10] Xiao, Y., X. Shen, B. Sun and L. Cai, 2006. “Security and privacy in rfid and applications in telemedicine”, IEEE Commun. Mag., 44(4): 64-72.