ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Design of Patient Self-Controllable healthcare System Expending Cloud Computing

Dr.K. Praveen Kumar

Associate Professor, School of Electrical Engineering & Computing, Department of Computing, Adama Science &Technology University, Adama, Ethiopia

ABSTRACT: Distributed m-healthcare structures assist for efficient affected patient treatment of excessive satisfactory, but it brings about collection of challenges in personal health information confidentiality and affected patient's identity privateness. Many present data access to control and anonymous authentication schemes inefficient in distributed m- healthcare systems. To solve the problem, in this paper, establish a unique legal on authorized accessible privacy model (AAPM) primarily based on this advice a affected patient self-controllable multi-degree privateness-maintaining cooperative authentication scheme (PSMPA). Distributed mhealthcare realizing 3 levels of protection and privacy requirement and patients can authorizes physicians by way of placing an get right of access to tree assisting flexible threshold predicates.

KEYWORDS: Authentication; access control; security and privacy; distributed m-healthcare; access tree

I. INTRODUCTION

Distributed m-healthcare cloud computing idea has emerged in latest years. We can say that it's far an affected patient centric model as universal control of patient's data is with patient. Due to the high cost of building and retaining facts facilities, third party service companies provide healthcare provider. But while using third party service provider there are many security and privateness risks inside the machine. In mhealthcare social networks, the non-public health data is usually shared among the patients placed in respective social communities suffering from the same sickness for mutual help, and across allotted healthcare providers equipped with their personal cloud servers for scientific consultant in dispensed m-healthcare cloud computing structures, which a part of the sufferers' non-public health information need to be shared and which health practitioner their personal fitness data ought to be shared with have emerge as intractable troubles annoying urgent solutions.

In latest years, the disbursed m-healthcare is emerged paradigm for exchanging the health data and lets in to create, manage and control her non-public health records, which has made the garage, retrieval, and sharing of scientific information extra efficient in cloud computing. The WHO defines the Mobile Healthcare is an area of the electronic fitness and it provide the heath data and offerings over cell technologies such as mobile phones and personal digital Assistants (PDAs).The personal health data is usually shared among the patient suffering from the identical disease, between the patients and physicians as equal opposite numbers or even throughout dispensed healthcare vendors for clinical consultant. This sort of personal fitness statistics sharing allows each collaborating healthcare company to method it regionally with higher performance and scalability, significantly enhances the remedy first-rate, notably alleviates the complexity at the patient side and therefore becomes the initial component of a dispensed m-healthcare device. However, it also brings about a series of challenges, particularly the way to ensure the safety and privateness of the patients' private fitness data from various attacks in the wireless communication channel together with eavesdropping and tampering. Main issue concerning the safety is the get admission to control of the affected person's personal statistics.

In dispensed m-healthcare cloud computing gadget, most effective the legal physicians or institutions that may recover the affected person's private statistics throughout data sharing. Most patients are concerned about the confidentiality in their private health data due to the fact it's far in all likelihood to cause them to in problem for each type of unauthorized collection and disclosure. For example, the patients' insurance software can be rejected once the

DOI: 10.15680/IJIRCCE.2016. 0410198

insurance company has the expertise of the severe fitness situation of its clients. Therefore, in allotted healthcare a machine, which part of the sufferers' non-public health records should be shared and which a part of physicians should their private health data be sharing is the primary hassle. Here, concurrently achieving each protection and confidentiality with excessive performance. In allotted m-healthcare systems, all the contributors may be classified into 3 categories:

- The at once authorized physicians who are legal with the aid of the patients,
- The circuitously authorized physicians who're authorized by means of the without delay authorized physicians for medical consultant or studies reason and
- The unauthorized humans.

In this paper, through extending the strategies of characteristic primarily based get admission to manipulate and exact verifier signatures on the recognized health information with the aid of realise three distinct levels of privateness-maintaining requirement: most effective the physicians at once legal by using the patients can access the patients'non-public health statistics and authenticate their identities simultaneously; the physicians and studies team of workers indirectly legal through patients can't authenticate the sufferers' identities however recover the private health information; at the same time as the unauthorized individuals can attain neither.

II. Related work

There exist a series of constructions for authorized accesscontrol of patients‟ personal health information As wediscussed in the previous section, they mainly study the issueof data confidentiality in the central cloud computingarchitecture, while leaving the challenging problem ofrealizing different security and privacy-preserving levels withrespect to (w.r.t.) kinds of physicians accessing distributedcloud servers unsolved. On the other hand, anonymousidentification schemes are emerging by exploitingpseudonyms and other privacy-preserving techniquesproposed SAGE achieving not only the content-orientedprivacy but also the contextual privacy against a strong globaladversary proposed a solution to privacy and emergencyresponses based on anonymous credential, pseudorandomnumber generator and proof of knowledge Lu et al. proposeda privacy-preserving authentication scheme in anonymousP2P systems based on Zero-Knowledge Proof However, theheavy computational overhead of Zero-Knowledge Proofmakes it impractical when directly applied to the distributedm-healthcare cloud computing systems where thecomputational resource for patients is constrained.

Misic andMisic suggested patients have to consent to treatment and bealerted every time when associated physicians access theirrecords Riedl et al. presented a new architecture ofpseudonymiaztion for protecting privacy in E-health (PIPE)Slamanig and Stingl integrated pseudonymization of medicaldata, identity management, obfuscation of metadata withanonymous authentication to prevent disclosure attacks andstatistical analysis in and suggested a secure mechanismguaranteeing anonymity and privacy in both the personalhealth information transferring and storage at a central mhealthcare cloud server Schechter et al. proposed ananonymous authentication of membership in dynamic groups. However, since the anonymous authentication mentionedabove are established based on public key infrastructure(PKI), the need of an online certificate authority (CA) and oneunique public key encryption for each symmetric key k fordata encryption at the portal of authorized physicians madethe overhead of the construction grow linearly with size of thegroup. Furthermore, the anonymity level depends on the sizeof the anonymity set making the anonymous authenticationimpractical in specific surroundings where the patients aresparsely distributed.

In this paper, the security and anonymity level of our proposedconstruction is significantly enhanced by associating it to theunderlying Gap Bilinear Diffie-Hellman (GBDH) problem andthe number of patients‟ attributes to deal with the privacy leakagein patient sparsely distributed scenarios in More significantly,without the knowledge of which physician in the healthcareprovider is professional in treating his illness, the best way for thepatient is to encrypt his own PHI under a specified access policyrather than assign each physician a secret key. As a result, theauthorized physicians whose attribute set satisfy the accesspolicy can recover the PHI andthe access control management also becomes more efficient.Last but not least, it is noticed that our construction essentiallydiffers from the trivial combination of attribute basedencryption and designated verifier signature. As the simulationresults illustrate, we simultaneously achieve the functionalitiesof both access control for personal health information andanonymous authentication for patients with significantly lessoverhead than the trivial combination of the two buildingblocks above. Therefore, our PSMPA far outperforms theprevious schemes in efficiently realizing access control ofpatients‟ personal health information and multi-level privacypreserving cooperative authentication in distributed mhealthcare cloud computing systems.

III.PROPOSED SYSTEM

The above mentioned schemes are not sufficient for efficiently processing the increasingthe volume of personal health informational and also not enough for to only guarantee thedata confidentiality of the patients personal health information in the honest-but-curiouscloud server model since the frequently communication between a patient and a physician.Overcoming of this problem, a novel authorized accessible privacy model (AAPM) isestablished. Patients can authorize physicians by setting an access tree supporting flexiblethreshold predicates. a patient self-controllable multi-level privacy-preserving cooperativeauthentication scheme (PSMPA) realizing three levels of security and privacy requirement indistributed m-healthcare system is proposed.

A. *SECURITY ARCHITECTURE*

In distributed m-healthcare systems, all the members can be classified into three categories:the directly authorized physicians, the indirectly authorized physicians, and unauthorizedpersons, this is showed in the Fig 1.The directly authorized physicians are identified with green labels in the local healthcareprovider they are authorized by the patients and these physicians can access the patient'spersonal health information and verify the patient's identity.The indirectly authorized physicians identified with yellow labels in the remote healthcareproviders they are authorized by the directly authorized physicians for medical consultant orsome research purposes. Since they are not authorized by the patients called 'indirectlyauthorized physicians'. They can only access the personal health information, but not the patient's identity.For the unauthorized persons identified with red labels, nothing could be obtained becauseno one can authorize directly or indirectly.

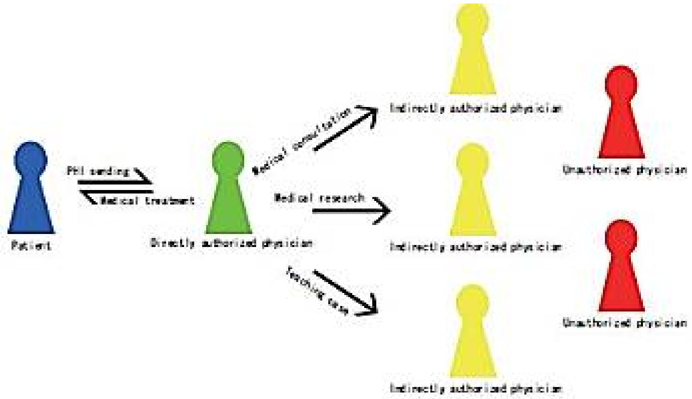

Fig 1: Multiple Security and Privacy Levels in m-Healthcare.

B. *APPLICATION SCENARIO IN PSMPA*

Consider the application scenario in PSMPA system shown in the Fig 2. Where all linksare bidirectional and the bracketed numbers indicate major events or exchanged messages.There are three distributed healthcare providers A, B, C and the medical research institutionD, where Dr. Brown, Dr. Black, Dr. Green and Prof. White are working respectively. Each ofthem possesses its own server.The patient P registers at hospital A, all her/his personal health information is stored inhospital A's server, and Dr. Brown is one of his directly authorized physicians. For medicalconsultation or other research purposes in cooperation with hospitals B, C and medicalresearch institution D, it is required for Dr. Brown to generate three indistinguishabletranscript simulations of patient P's personal health information and share them among thedistributed cloud servers of the hospitals B, C and medical research institution

D.The internal links of the hospital/clinic network and the patient LAN are often high-speedwired links. The patient interacts with the family and P-device to assign privilege (i.e., secretkeys) that will be used for retrieving the patient's PHI in emergencies.

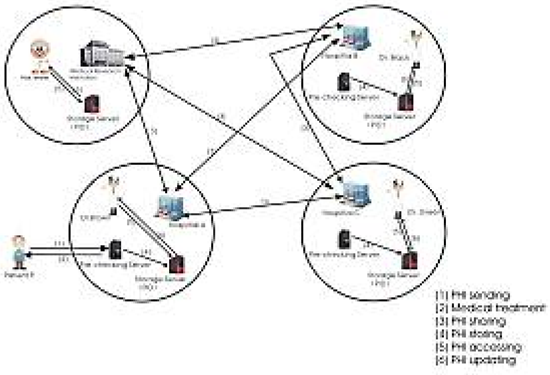

Fig 2: An Overview of Our Distributed m-Healthcare

IV.CONCLUSION

In this paper, a novel authorized accessible privateness model (AAPM) and a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSCPA)knowing three special levels of protection and privacy requirement inside the allotted mhealthcare cloud computing device are proposed and additionally averted the a number of the attackshappened within the wireless communication medium.

REFERENCES

[1] L.Gatzoulis and I. Iakovidis, Wearable and Portable E-health Systems,IEEE Eng. Med. Biol. Mag., 26(5):51-56, 2007.
[2] I. Iakovidis, Towards Personal Health Record: Current Situation, Obstacles and Trends in Implementation of Electronic Healthcare Recordsin Europe, International Journal of Medical Informatics, 52(1):105-115,1998.
[3] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, A NewSolution for A Heart Failure Monitoring System based on Wearable andInformation Technologies, In International Workshop on Wearable andImplantable Body Sensor Networks 2006-BSN 2006, April, 2006.
[4] R. Lu and Z. Cao, Efficient Remote User Authentication Scheme UsingSmart Card, Computer Networks, 49(4):535-540, 2005.
[5] M.D.N. Huda, N. Sonehara and S. Yamada, A Privacy Management Architecture for Patient-controlled Personal Health Record System, Journalof Engineering Science and Technology, 4(2):154-170, 2009.
[6] S. Schechter, T. Parnell and A. Hartemink, Anonymous Authentication ofMembership in Dynamic Groups, in Proceedings of the Third InternationalConference on Financial Cryptography, 1999.
[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry,Anonymity and Application Privacy in Context of Mobile Computing ineHealth, Mobile Response, LNCS 5424, pp. 148-157, 2009.
[8] M. Li, S. Yu, W. Lou and K. Ren, Group Device Paring based SecureSensor Association and Key Management for Body Area Networks, InIEEE Infocom 2010.
[9] S. Yu, K. Ren and W. Lou, FDAC: Toward Fine-grained Distributed DataAccess Control in Wireless Sensor Networks, In IEEE Infocom 2009.
[10] F.W. Dillema and S. Lupetti, Rendezvous-based Access Control forMedical Records in the Pre-hospital Environment, In HealthNet 2007.
[11] J. Sun, Y. Fang and X. Zhu, Privacy and Emergency Response in Ehealthcare Leveraging Wireless Body Sensor Networks, IEEE WirelessCommunications, pp. 66-73, February, 2010.
[12] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, SAGE: A StrongPrivacy-preserving Scheme against Global Eavesdropping for E-healthSystems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.
[13] J. Sun, X. Zhu, C. Zhang and Y. Fang, HCPP: Cryptography BasedSecure EHR System for Patient Privacy and Emergency Healthcare,ICDCS'11.
[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 Transactionson Parallel and Distributed Systems, vol. 19, No. 10, October, 2008.
[15] J. Zhou and M. He, An Improved Distributed key Management Scheme inWireless Sensor Networks, In 9th. International Workshop of InformationSecurity Applications 2008-WISA 2008, September, 2008.

DOI: 10.15680/IJIRCCE.2016. 0410198

BIOGRAPHY

Dr.K.Praveen Kumarreceived the PhD in Computer Science & Engineering in 2015, M.Tech in Software Engineering from Kakatiya Institute of Technology & Science Warangal, Telangana, India in 2010 and B.Tech in Information Technology from Kakatiya Institute of Technology & Science Warangal, Telangana, India 2007. Presently working as Assistant Professor in Computer Science Department at Adama Science and Technology University, Adama, Ethiopia.

DOI: 10.15680/IJIRCCE.2016. 0410198