|| Volume 1||Issue||Aug 2016||ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

HEALTHCARE IN CLOUD USING MULTI-LEVEL PRIVACY-PRESERVING PATIENT SELF-CONTROLLABLE ALGORITHM

Syed imrana Fatima[1] , Saad Siddiqui[2]

Student, Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, India[1]

Asst.Prof, Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, India[2]

***Abstract* :- Secure patients' confidentiality and privacy preserving healthcare system is well proposed which makes access control of the vital healthcare information of the personals using it in this case it is the patients. In order to solve this problem a scheme as PSMPA was proposed to take care about the data and information of the personnel. Patients can consent to physicians by setting an access tree sustaining flexible threshold predicates. This scheme will be using DVS and ABE algorithms in order to realize security and privacy. This is supposed to be realized in a distributed environment. The basic aim of the scheme is to provide the access rights control in the hand of patients so that they can manage their personnel healthcare information which can otherwise if seized by intruders can be used for breach of privacy of the patient.**

I INTRODUCTION

Cloud computing is a new and emerging paradigm for distributed computing, which allows to provide storage, computing powers as well as software and platform for development of software on an on demand basis or else by reserving resources on the cloud. This is fulfilled by some SLA agreements between the service providers and the users of the setup[11]. The concept is to commodity the computing functionalities and make it available as a commodity to the users whenever wherever required. Conceptually similar to power or electricity supply quite much. The services provided by cloud computing can be largely categorized as 'Infrastructure as a Service' (IaaS), in which infrastructure is provided as a service by the cloud service provider 'Platform as a Service (PaaS)' e.g. aneka which provides platform as a service for the developers or 'Software as a Service' (SaaS)[3]. Clients can right to use web-based tools or applications in the course of a web browser or using a cloud-based resource like storage or computer power like installed locally, eliminating the requirement to install as well as run the application on the customer's personal computer and this well also help in making the maintenance easier.

The cloud can be developed as any of the following

1. Private cloud: This contained within the organization.
2. Public cloud: can be assessed by people outside the organization also.[5]
3. Hybrid cloud: this is amalgamation of the above two.

Healthcare industry has as compared to other industries, has not utilized emerging technology in order to increase its operational abilities[8]. Many healthcare organizations still rely on paper medical account, report. Data information that is digitized is characteristically not transportable, which restricts knowledge sharing between the different healthcare providers. Utilization of technology to smooth the progress of association and to synchronize heed between patients and medical practitioners, and amongst the medical society is inadequate. There is a need for modernization of healthcare information technology (HIT) which can be facilitated with the utilization of the computing powers of cloud computing giving ease of deployment of applications and significantly very less initialization cost[10]. Cloud computing is capable enough to bring about revolutionary change in the way data is handled in healthcare organizations. The healthcare organizations are changing in the direction of an information-centric model, by open principles that sustain collaboration, shared workflows and information distribution. Cloud computing fulfills the foremost technology necessities of the healthcare industry: by providing on-demand admittance to computing and large storage conveniences which otherwise was not facilitated in legacy healthcare software. Maintenance of huge amount of data sets for electronic health records (EHR), radiology images and genomic data offloading, is also possible in cloud platform which otherwise would be a big aggravate[4].

The main concern is the integrity and privacy of personnel heath care information of the patients, the intent of the proposed system is to provide the control of information to the patients they themselves, the benefit of the proposed system will be as follows

1. Sharing of EHRs among authorized medical practitioners and research centers in various geographically distributed areas,

2. Providing access to practitioners for second opinion and reference

3. Provide authorization rights in the hands of the patients improves the reliability of information passage in the EHRs (with the proper information governance).

Table 1.The basic comparisons between Paper-based and Electronic-based PHR

PHR class Property	Paper-based PHR	Electronic based PHR
Availability	Hardcopy	softcopy
accessibility	locally	globally
protection	open	secure
Update	difficult	Easy
storability	On paper	On electronic storage

The biggest hindrances in using a cloud based system for the PHR in that the control of information goes into the hands of the third party cloud service providers; this holds back the clients to trust such kind of systems in terms of data storage and management. Personnel Healthcare data has stern requirements for confidentiality, security, availability to authorized patients [6]. Clouds vendors need to note this accordingly develop some SLA agreements with the users, while also taking into consideration legal issues pertaining to the government and industry regulations. Challenges in Healthcare for migrating into Cloud Computing Information technology can be explored in order to get the benefits of the ever evolving technological advancements in information communication systems (ITC)[5]. New and improved facilities can be provided to the users or the patients. The basic concern remains the same as of privacy, reliability security, incorporation and data portability. Privacy and Security Challenges Data managed in a cloud contain private and confidential, personnel information such as regarding a particular ailment the person might be suffering from, this information if goes into the hands of say Health Insurance Company; it might adversely affect the chances of that person being able to get the health insurance. Cloud Computing for Healthcare Keeping the patient in-charge of his personnel health care data is the main motive in the current cloud offerings. This gives the user the control over his confidential data by not compromising on the clinical support by the peers.

II SYSTEM ARCHITECTURE

In the proposed distributed system members or actors are divided into three levels depending on their access rights over the health care information

1. Directly access rights
2. Indirect access rights
3. No rights

The first type of actors can access both the personnel health care information as well as the patient profile, the second set of actors can see the healthcare information but cannot access the patient profile, these are the physicians who can read only the medical condition and respond on the same. The third type of actors cannot view any the health data or the patient profile.

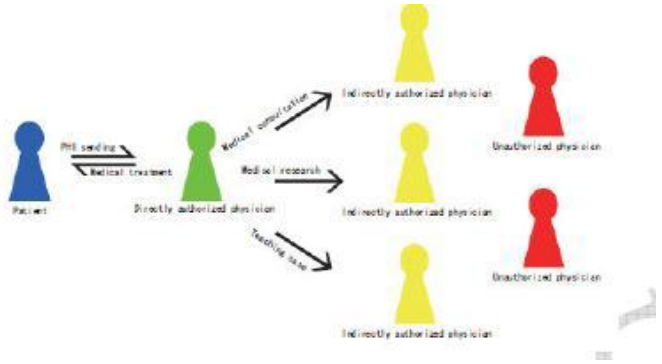

Figure 1. Multiple Security and Privacy Levels in m-Healthcare

In the above figure the red icons belong to the third category, the yellow icons belong to the second category and the green icons belong to the first category. The information access for the first type of actor is provided by the patient. The access for the second type of actor is provided by the type one actor. The basic scheme in order to realize the same is.

An authorized accessible privacy model for the multi-level access approach to be realized with different kind of access rights to the physicians in distributed framework is is incorporated for the generation of the (PSMPA) scheme known as the patient self-controllable multilevel privacy-preserving cooperative authentication scheme for the confidentiality, privacy, security of the data. More so ever we use the combination of (ABE) technique and designated verifier signature (DVS). Attribute-based encryption is a category of public-key encryption. In ABE secret key of a patient and the ciphertext relative to the query are reliant upon attributes (e.g. the kind of subscription). The decryption of a ciphertext is accomplished only if the set of attributes of the user key matches the attributes of the

ciphertext[15]. Designated verifier signature (DVS) is a cryptographic methodology in which there is a provision of the signer to induce a verifier the legitimacy of a testimonial such that the verifier is incapable to reassign the confidence to a third person[16].

In DVS, signatures are visibly confirmable. If it is from the signer or the verifier then only it is considered as valid.

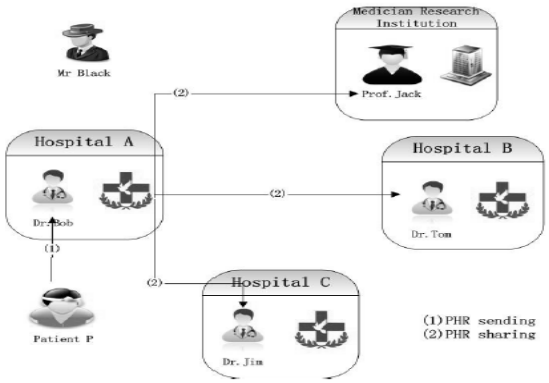

Figure2: An Overview of Our Distributed m-Healthcare System

Figure 2, shows a instance of the health care system. As illustrated in the figure actors are divided into 3 levels of security based on their access rights. Patient is meeting the physician bob, whom we call as the local health care provider he given the direct access right by the patient. Tom, jack and jim are at a geographically remote location and are not having direct access to the patient heath care information, bob can give access to the indirect access physicians. If bob does not give access right to jack then jack will not be able to see the personnel profile of patient neither the health related data.

IV CONCLUSION

There is a void of technological advancement in the field of medical science in India. Technology can ensure easy and fast access to the information, rapid sharing of data is also possible especially for the medical research purpose.

Healthcare organization have a bright future in Cloud computing. The initialization cost is minimized in clouds. There is provision of scalability, elasticity which promote such advancements. Any time sharing of data to geographically diverse location is possible in such a distributed environment.

The data being patient self controllable gives him the reliance that there will not be any misuse of his personnel health record.

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 Inplementation of Electronic Healthcar Records in Europe*, International Journal of Medical Informatics,52(1):105-115, 1998.

[3] 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 International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[4] R. Lu and Z. Cao, *Efficient Remote User Authentication Scheme Using Smart 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*, Journal of Engineering Science and Technology, 4(2):154-170, 2009.

[6] S. Schechter, T. Parnell and A. Hartemink, *Anonymous Authentication Membership in Dynamic Groups*, in Proceedings of the Third International Conference 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 in eHealth*, Mobile Response, LNCS 5424, pp. 148-157, 2009.

[8] J. Zhou and Z. Cao, *TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks*, In IEEE Globecom 2012.

[9] S. Yu, K. Ren and W. Lou, *FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks*, In IEEE Infocom 2009.

[10] F.W. Dillema and S. Lupetti, *Rendezvous-based Access Control for Medical 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 Wireless Communications, pp. 66-73, February, 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 Journal on Selected Areas in Communications, 27(4):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*, 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 Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, October, 2008.

[15] J. Zhou and M. He, *An Improved Distributed Key Management Scheme in Wireless Sensor Networks*, In WISA 2008.

[16] 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.