Efficient Attack Prevention Method for Protecting Electronic Health Records (EHRs) in Cloud

V.M.Prabhakaran[1], Prof.S.Balamurugan[2], S.Charanyaa[3]

PG Scholar, Department of CSE, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1]

Assistant Professor, Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[2]

Senior Software Engineer Mainframe Technologies Former,Larsen& Tubro (L&T) Infotech,Chennai TamilNadu, India[3]

Abstract: The usage of cloud computing for storage and retrieval of electronic health records(EHRs) have seen a steep rise in past few years. This paper proposes an efficient attack prevention mechanism from unauthorized user to the electronic health records stored in cloud. Also effective secured electronic health record retrieval mechanism is also proposed. Health record signals are been stored and processed for the predetermined health function or parameter to define value in the abnormal range. Also future health signal record is to trend the predetermined function and assume a value in abnormal range and condition. PHR systems typically offer functionality to share, visualize and analyze PHR data. Secure lifelong management of patient medical records since data are stored in the cloud and do not have to be carried around by patients.

Keywords: Electronic Health Records (PHRs), Attack Prevention, Retrieval Mechanism, Medical Record, Cloud Computing

I. INTRODUCTION

Cloud storage services to users, where users can have access to very large volume of storage. Data kept on clouds can also be shared by users giving that the sharing is authorized by the data owners Alice has a piece of data that is kept on the cloud. Secure data sharing needs to be achieved via an un trusted cloud storage provider. It is necessary that the cloud storage provider helps to enforce the authorization policy for data access but the enforcement should not reveal any information to the cloud storage provider or enable the cloud storage provider have excessive privileges to allow unauthorized access.Cloud storage services provide, very large volume of storage to outsource user data. Data kept on clouds can also be shared to users that the sharing is authorized by the data owners. Cloud storage provider helps to enforce the authorization policy for data access.

The remainder of the paper is organized as follows. Literature review of several techniques prevailing in literature aimed to secure the electronic health records in recent years are discussed in Section 2. The detailed architectural framework is depicted in Section 3. Section 4 details about attack prevention mechanisms from unauthorized users. The strategy for secured retrieval mechanism from authorized users is discussed in Section 5. Section 6 concludes the paper and outlines the direction for future work.

II. LITERATURE SURVEY

Arindam Banerjee, PrateekAgrawal and R. Rajkumar (2013) [15] in "Design of a Cloud Based Emergency Healthcare Service Model" explored that Cloud computing plays an important role in medical field and Information technology for most scalable and resources satisfy the customer needs. Virtual health service is a remote based patient monitoring system which serves patients in emergency condition. Previous medical history can also be retrieved and analyzed for future process. Every system or process is integrated with unique identification number systems.

Louise Olsson, Gunnel Östlund, Peter Strang, Eva JeppssonGrassman, Maria Friedrichsen (2010) [16] in "Maintaining hope when close to death: insight from cancer patients in palliative home care" explored that cancer patients receiving palliative home care used to keep their hope alive, use a grounded theory methodology. Two important processes are evolved maintaining life and preparing for death. Proposed and revealed two parallel and interdependent processes used by patients in the palliative care phase to uphold hope and respond to living close to death.

K.S. Aswathy, G. Venifa Mini (2014) [17] in "Secure Alternate Viable Technique of Securely Sharing the Personal Health Records in Cloud" defined in cloud computing environment resources can be accessed in free also pay per use process. It provides different kinds of services and framework. Personal health record sharing is an important in that, share the data but some issues occur such as data loss, third party interfere. To overcome all those shortcomings secure alternative viable technique is proposed which overcome problem of security issues.

Jithendra K, Thanapal P, Prabhu J (2013) [18] "Developing Secure Social Healthcare System over the Cloud" defined two important technologies in current such as Social media and cloud computing. Evolving and upholding a healthcare system with self-infrastructure well cost more. Small institutions have hard copy of records. Healthcare application will provide web service which is established over the cloud so it well decreases the cost and

they need not be concerned about infrastructure. Cloud providers well software which update frequently. Since data is exist in the cloud, security may be main concern to be concerned.. By using role based access control healthcare system is secured.

L G Branch and A M Jette (1984) [19] "Personal health practices and mortality among the elderly. American Journal of Public Health" defined that Morality is reduced between personal health practices. They inspected the association of physical activity, cigarette smoking, hours of sleep, alcohol consumption, and number of meals with five-year mortality rates.The personal health practices are related significantly to mortality among elderly men.

Jean Harvey-Berino, Stephen Pintauro, Paul Buzzell, and Elizabeth Casey Gold (2004) [20] in "Effect of Internet Support on the Long-Term Maintenance of Weight Loss" objective are to examine the effectiveness of an Internet weight maintenance program. Members assigned to an internet-based weight maintenance program sustained comparable weight loss. Therefore, the internet appears to be a viable medium for promoting long-term weight maintenance.

III.ARCHITECTURAL FRAMEWORK

The architectural representation of cloud based PHR storage is represented in Fig 1. The portal plays an important role in uploading copy of data, remote access maintenence, start/stop operation. PCAS access is used to provide and show copies. The cloud takes the responsibility of mounting the PHRs.
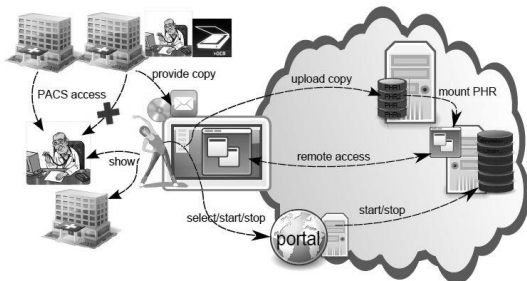

Fig. 1. Architectural example Cloud Based PHRs storage

Architectural representation of MyPHR Machine consists of two components evolution and storage with which client directly interacts with MyPHR Machine. The first component of MyPHR Machine consists of web portal which in turn interacts with Virtual Box Hypervisor. Virtual Machines are connected together with Virtual Box Hypervisor. The second component of MyPHR Machine, storage consists of VM Repository which houses VM Data and Private Network folders as indicated in Figure 2.

IV.PREVENTION MECHANISM FROM UNAUTHORIZED USER

Once stored in Cloud environment, patients can flexibly view and share these data with any other care institution or interested stakeholder. Cloud environment also allows care institutions to make available specialist software required to view or analyze health data. When the Cloud user three upload a copy of the medical data of the relevant patient to whom the bonding has been given, Only the same relevant patient can view the medical data which has been
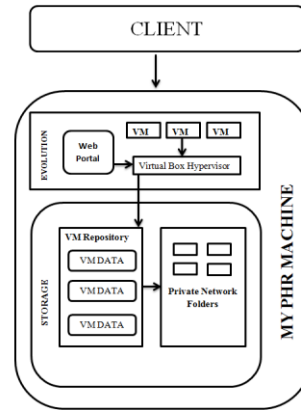

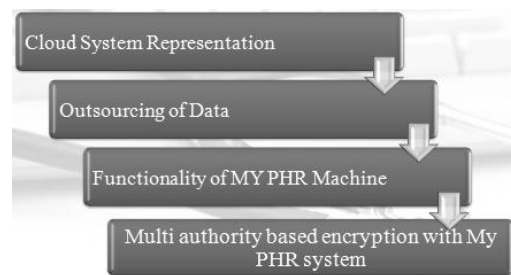Fig. 2. Technical Architectural diagram of Cloud Based PHRs storage

Fig. 3. Modular Workflow of Cloud Based PHRs storage

uploaded, the user is provided with authorization functionality toprocess the data so to outsource the user have to enroll the cloud user as three in the outsourcing function. But in some case unauthorized users involve in accessing the specified user data for knowing the medical details which was kept in confidential manner, but it can't be visible because the data viewing functionality is provided only for the specified doctor and the patient. This fact is illustrated in Fig 4.

Fig 4: Prevention from the unauthorized user

V. SECURED RETRIEVAL MECHANISM FROM AUTHORIZED USER

Also in some process the cloud user can two try to outsource the data of the cloud user three, But it ends in fail they can't access they get information such as This level user don't have permission to access the data. So the privacy information of the patient data is been protected. This fact is illustrated in Fig 5.
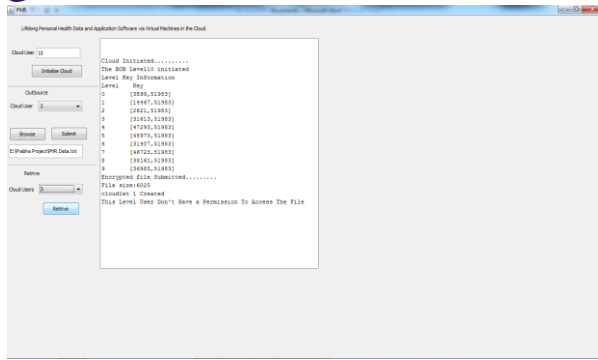
Fig 5: Retrieval of patient data with the authorized user

VI. CONCLUSION AND FUTURE WORK

This paper proposed an efficient attack prevention mechanism from unauthorized user to the electronic health records stored in cloud. Also effective secured electronic health record retrieval mechanism is also proposed. Health record signals are been stored and processed for the predetermined health function or parameter to define value in the abnormal range. Also future health signal record is to trend the predetermined function and assume a value in abnormal range and condition. PHR systems typically offer functionality to share, visualize and analyze PHR data. Secure lifelong management of patient medical records since data are stored in the cloud and do not have to be carried around by patients. As a part of future work, we have planned to design and implement secure data retrieval mechanisms from cloud.

REFERENCES

[1] Pieter Van Gorp and Marco Comuzzi "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud" IEEE Journal of Biomedical and Healthcare Informatics, Vol. 18, No. 1, Jan 2014

[2] Pieter Van Gorp and Marco Comuzzi (2014) Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud, IEEE Journal of Biomedical And Health informatics.
    Richard Lenz, Manfred Reichert (2006) IT support for healthcare processes– Premises, challenges and perspectives, Elsevier.

[3] GoceGavrilov, Vladimir Trajkovik (2012) Security and Privacy Issues and Requirements forHealthcare Cloud Computing, ICT Innovations 2012 Web Proceedings

[4] Sean M. Randall Anna M. Ferrante, James H. Boyd, James B. Semmens (2013) ,Privacy-preserving record linkage on large real world datasets, Elsevier.

[5] J. Vidhyalakshmi, J. Prassanna (2012) Providing a trustable healthcare cloud using an enhanced accountability framework.

[6] M. Poulymenopoulou, F. Malamateniou, D.Papakonstantinou , G. Vassilacopoulos (2011) Cloud-based Information Support forEmergency Healthcare.

[7] William R. Hogan, MD, Michael M. Wagner, MD, PHD (1997) Accuracy of Data in Computer-based Patient Records .

[8] Laurence G.Branch, PHD (1985) Health Practices and Incident Disability among the Elderly, Public health briefs.

[9] Eleanor M. Simonsick, PhD, Mary E. Lafferty, Caroline L. Philips, MS,Carlos F. Mendes de Leon, PhD, Stanislav V Kasl, PhD, Teresa E.Seeman, PhD, GerdaFillenbaum, PhD, Patricia Hebert, PhD, and Jon H.Lemke, PhD(1993) Risk Due to Inactivity in Physically Capable Older Adults, American journal of public health.

[10] Robert Steele, Kyongho Min, Amanda Lo (2012) Personal Health Record Architectures: Technology Infrastructure Implications and Dependencies.

[11] HebahMirza and Samir El-Masri, Cloud Computing System for Integrated Electronic Health Records.

[12] Abhishek Kumar Gupta, Kulvinder Singh Mann (2014) Sharing of Medical Information on Cloud Platform-A Review, IOSR Journal of Computer Engineering**.**

[13] Carmelo Pino and Roberto Di Salvo (2013) A Survey of Cloud Computing Architecture and Applications in Health, International Conference on Computer Science and Electronics Engineering.

[14] Peter L. Reichertz (2006) Hospital information systems - past, present, future, International Journal of Medical Informatics.

[15] Arindam Banerjee, PrateekAgrawal and R. Rajkumar (2013) Design of a Cloud Based Emergency Healthcare Service Model, International Journal of Applied Engineering Research.

[16] Louise Olsson, Gunnel Östlund, Peter Strang, Eva JeppssonGrassman, Maria Friedrichsen (2010) Maintaining hope when close to death: insight from cancer patients in palliative home care.

[17] K.S. Aswathy, G. Venifa Mini (2014) Secure Alternate Viable Technique of Securely Sharing the Personal Health Records in Cloud, International Journal of Recent Development in Engineering and Technology.

[18] Jithendra K, Thanapal P, Prabhu J (2013)Developing Secure Social Healthcare System over the Cloud, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[19] L G Branch and A M Jette. Personal health practices and mortality among the elderly. American Journal of Public Health.

[20] Jean Harvey-Berino, Stephen Pintauro, Paul Buzzell, and Elizabeth Casey Gold (2004) Effect of Internet Support on the Long-Term Maintenance of Weight Loss.

[21] Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013

[22] Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.

[23] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014

[24] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014

[25] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014

[26] S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014.

BIOGRAPHIES

V.M.Prabhakaran obtained his B.E. degree in Computer Science and Engineering from Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India and currently pursuing his M.E. degree in M.Tech degree in Computer Science and Engineering at KalaignarKarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. He has to his credit **17 papers** in National/International Journals/Conferences.

He is the recipient of **gold medal and certificate of merit for best journal publication** by his host institution for the year 2013-14. He served as a **Secretary** for CSE Association at Hindusthan Institute of Technology, 2011-12. He currently holds the position of student **President** for CSE Association, KalaignarKarunanidhi Institute of Technology. He has secured a **best paper award in an International Conference** held at Coimbatore Institute of Technology, Coimbatore, TamilNadu, India. His areas of research interests include Network Security, Cloud Computing and Database Security.

Prof.S.Balamurugan obtained his B.Tech degree in Information Technology from P.S.G. College of Technology, Coimbatore, Tamil Nadu, India and M.Tech degree in Information Technology from Anna University, Tamil Nadu, India respectively. He is currently working towards his PhD degree in Information Technology at P.S.G. College of Technology, Tamil Nadu, India. At present he holds to his credit **58 papers International Journals and IEEE/ Elsevier International Conferences.** He is currently working as Assistant Professor in the Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India affiliated to Anna University TamilNadu, India. He is **State Rank holder** in schooling. He was **University First Rank holder** M.Tech. Semester Examinations at Anna University, Tamilnadu, India. He served as a Joint Secretary of IT Association, Department of Information Technology, PSG College of Technology, Coimbatore, Tamilnadu, India. He is the **recipient of gold medal and certificate of merit** for best journal publication by his host institution **consecutively for 3 years**. Some of his professional activities include invited Session Chair Person for two Conferences. He has guided 12 B.Tech projects and 2 M.Tech. projects. He has won a best paper award in International Conference. His areas of research interest accumulate in the areas of Data Privacy, Database Security, Object Modeling Techniques, and Cloud Computing. He is a life member of ISTE,CSI. **He has authored a chapter in an International Book "Information Processing" published by I.K. International Publishing House Pvt. Ltd, New Delhi, India, 978-81-906942-4-7. He is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**

S.Charanyaa obtained her **B.Tech** degree in Information Technology and her **M.Tech** degree in Information Technology from Anna University Chennai, Tamil Nadu, India. She was **gold medalist** in her B.Tech. degree program. She has to her credit **20 publications in various International Journals and Conferences**. Some of her outstanding achievements at school level include **School First Rank holder** in **10th and 12th grade**. She was working as Software Engineer at Larsen & Turbo Infotech, Chennai for 3 years where she got promoted as Senior Software Engineer and worked for another 2 years. She worked at different verticals and worked at many places including Denmark, Amsderdam handling versatile clients. She is also the recipient of **best team player award for the year 2012 by L&T**. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Cloud Computing. **She is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**