ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

Effective Key Generation for Outsourcing Personal Health Records (PHRs) 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: Recent days have seen an increased concern in securing data stored in cloud. Cloud computing, besides providing a maximized effectiveness of shared resources, also provides an easy way of storing and retrieving data. Personal Health Records (PHRs) are designed to maintain lifelong details of patients. Automated Patient Identifier and Patient Care System is designed to count hospitalized patients based on the concept of Current Procedure Terminology (CPT) manager. Cloud storage service is accessed through the cloud computer service, web service application programming interface or by a cloud storage gateway. The cloud based workspace is centralized providing easy functionality to share. The cloud environment can provide improvements in system efficiency & density. This paper invades the architecture and initialization of cloud to host patients' medical history. Also this paper, addresses the issue of outsourcing of data in cloud by the method of key generation for cloud user.

Keywords: Cloud Computing, Personal Health Records (PHRs), Key Generation, MyPHRMachines, Web service application program interface

I. INTRODUCTION

In the present world people suffer from various health problems. They frequently go to different hospitals to get guidance and get their treatments. However they also hurt from health problems they do not wish to share with anyone about their health problems and treatments. So they are in need of a new system to know about their health conditions. Cloud environment provides one such service. Cloud Computing has been intended as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. When the information is maintained in cloud it has various advantages patient no need to carry medical records where ever they go they can access from any desired place. It also minimizes the stress of the patient and the time.

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 basic primitives and terminologies are depicted in Section 3. Section 4 gives the architectural representation of cloud based PHR storage systems. Section 5 briefs about the process of Initializing the cloud. Outsourcing mechanisms of data in cloud is discussed in Section 6. Section 7 concludes the paper and outlines the direction for future work.

II. LITERARY REVIEW

Pieter Van Gorp and Marco Comuzzi (2014) [1] proposed "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud" defined a cloud based Personal Health Records (PHR) which stores the patient medical history of a patient for lifelong. They propose a prototype MY PHR machine, Caregiver or Institution upload the patient data in My PHR Machines. Once they upload the copy, Patient can view their medical data also patient have the capability to share their medical data to the selected caregiver they share through the remote machine. They applied to two use cases radiology image sharing and personalized medicine. Data kept on cloud are more secure and the implementation of this process results in new architectural solution to health record portability.

Richard Lenz, Manfred Reichert (2006) [2] in "IT support for healthcare processes– Premises, challenges and perspectives" proposed that Cooperation is an important factor for healthcare process, whereas optimal process is difficult to handle. Proposal of this paper states that elaboration of both potential and limitations of IT support for healthcare process. We adopt a broad Socio-technical perspective based on scientific literature and personal experience to identify the restrictions of IT support. It also expose the idea of the advance process management technology to improve IT support for healthcare processes.

GoceGavrilov, Vladimir Trajkovik (2012) [3] defined "Security and Privacy Issues and Requirements forHealthcare Cloud Computing" explore that IT is mostly used in healthcare in process to improve the medical services and also involved in deduction of cost. Electronic Health Record (EHR) is widespread building a secure environment for health care industry. Cloud computing is the popular infrastructure for sharing and integrating the Electronic health records. They involved in sharing the medical records and data whenever or wherever needed. Through cloud it's easy to access the medical data which serves as an improvement in the business models. Security and privacy issue is also an important factor, here they focus on the security and privacy and requirement process and improve the Healthcare IT system.

Sean M. Randall Anna M. Ferrante, James H. Boyd, James B. Semmens (2013) [4] in "Privacy-preserving record linkage on large real world datasets" explore that personal identity information linkage involves in use of dedicated linkage units to define individuals from datasets. Information supplied to linkage datasets reduces the risk of leak of sensitive information. Here the proposal called Record linkage which involved in reducing the privacy risks. This method uses bloom filters that are encrypted personal identifying information in a probability based linkage framework. Focused on possibility of privacy preserving linkage of large data sets. Also By using the bloom filter process to encrypt and compare separable fields, along with a Probabilistic linkage framework, large scale privacy preserving linkage can occur at no cost to linkage quality. Finally we can improve the healthcare privacy data.

J. Vidhyalakshmi, J. Prassanna (2012) [5] proposed "Providing a trustable healthcare cloud using an enhanced accountability framework" explored that Security and accountability of patient's personal health record maintenance it handle the Privacy protection problem. They define Distributed accountability framework to control and monitor user data in cloud. It also handle the object centric which automatically trigger an object to create a log record and access over distributed data. Log file corruptions are handled, log manager maintenance and verify corrupted log records. With the introduction of cloud computing in medical data capital expenditure is converted to operational expenditure.

M. Poulymenopoulou, F. Malamateniou, D.Papakonstantinou , G. Vassilacopoulos (2011) [6] in "Cloud-based Information Support for Emergency Healthcare" explored that ubiquitous access to integrated patient information is measured as important for making appropriate emergency healthcare plans. Scalable service oriented architecture is defined and through cloud computing they manage the patient information in a distributed and ubiquitous manner.

III. Basic Primitives And Terminologies

Cloud environment may describe a company, organization or an individual who uses a Web based application for every mission rather than installing software and storing data on a computer. Cloud environment involves in provide a functionality to outsource and encrypt the data. Cloud storage service is accessed through the cloud computer service, web service application programming interface or by a cloud storage gateway. The cloud based workspace is centralized providing easy functionality to share. The cloud environment can provide improvements in system efficiency & density. Cloud environment solve the problem of complicated configuration management, Decreased productivity, Limited accessibility and Poor collaboration. It has the capability to access all work, databases and other information from any device. Cloud environment involves in providing some basic network model for storage of data in the cloud.

The basic network model for the cloud data storage and three different network entities are

1. User
2. Cloud storage server
3. Cloud service provide

a. **User**: An entity which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation can be either individual consumers or organizations.

b. **Cloud Storage Server (CSS)**: An entity which is managed by Cloud service provider. Cloud storage is a subgroup of cloud computing. Cloud computing organizations offer users access to not only storage, but also processing power and computer applications mounted on a remote network. Cloud storage provides users with instant access to a wide ranging of resources and applications hosted in the infrastructure of another organization through a web service interface. Security of stored data and data transfer may be a concern during storing the sensitive data at a cloud storage provider.

c. **Cloud Service Provider (CSP)**:A cloud provider is a company that compromises some constituent of cloud computinghas significant storage space and computation resource to maintain the user data. The Data owner encrypted some keywords about his data, and service provider supported the owner to retrieve his data by keywords and not allow others to retrieve. When supposing the role of cloud provider, an organization is accountable for making cloud services available to cloud customers.

IV. Architectural Representation

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.

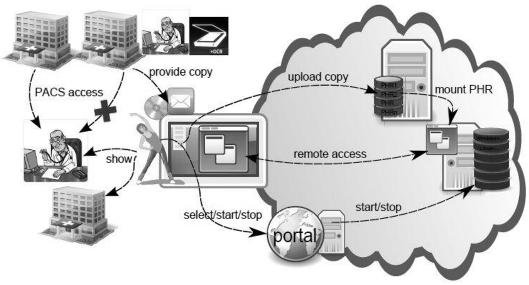


Fig. 1. Architectural example Cloud Based PHRs storage

V. Initialization Of Cloud

A PHR (Personal Health Record) is a health record which contains the health data and the information related to the care of a patient is maintained. It is a computer based tools that to access and organize their lifelong health data and make suitable parts of it available to those who need it.PHR (Personal Health Record) have the prospective to help examine an individual's health profile and classify health threats and improvement chances based on an examination of drug collaboration, gaps in medical care plans, best medical practices and identification of medical faults. Patient illnesses can be tracked in combination with healthcare providers and early interventions can be stimulated upon meeting deviation of health status. PHRs also make it easier for Institutions to care for their patients by assisting continuous communication as opposed to discontinuous. A cloud can be initialized by the owner such as Doctor or some organizations who involved in handling the record of a patient. First step is the process of starting up a program. Cloud server specifies the Initiator or Owner name that is responsible to upload the data of a particular patient in the cloud environment.

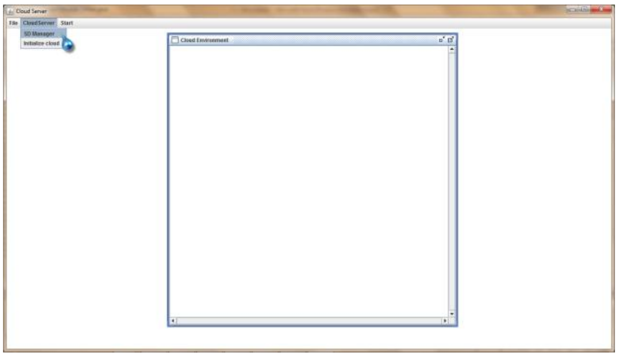
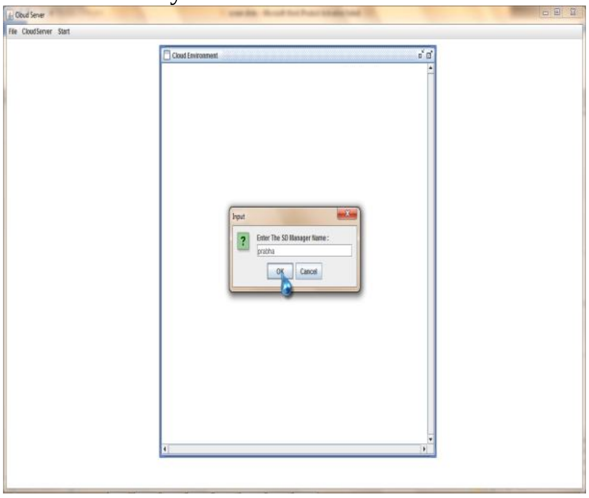


Fig 3: Cloud server Specification

After enrolling the name Owner of the data can initiate the cloud to access the cloud environment. Thus Initialization is the process of locating and using the defined values. The person or organization that officially maintains a cloud service is called a cloud service owner. The cloud service owner can be the cloud consumer or the cloud provider that owns the cloud within the cloud service localization. Enrolling the Initiator name specifies that which owner or the organization involved in outsource the Patient data. There can be several number of cloud users in cloud environment to optimize the cloud resource Cloud server initiator name is functionalized for better functionality of cloud service.

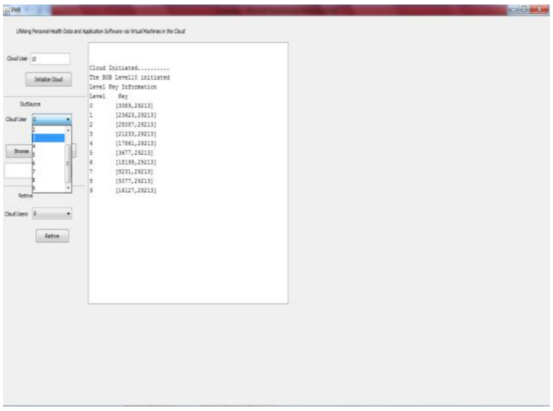


Enter The SD Manager Name : prabha

Fig 4: Enrolling the Initiator name

VI. OUTSOURCING OF DATA IN CLOUD

The Data which is being monitored and analysed by the Data owner such as doctor or Organization involved in Outsourcing the patient data in cloud which helps the patient to access their health record details at any place also at any time. Before outsourcing the data in cloud user have to initiate the cloud and Start the outsourcing application.


PHR
Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud
Initialize Cloud
OutSource
Browse
Retrive
Retrive

Cloud User 10

```
Cloud Initiated.........
The BOB Level10 initiated
Level Key Information
Level    Key
0        [3589,29213]
1        [25623,29213]
2        [28087,29213]
3        [21233,29213]
4        [17861,29213]
5        [3677,29213]
6        [18199,29213]
7        [8231,29213]
8        [5077,29213]
9        [16127,29213]
```

Cloud User 0

Cloud Users 0

Fig 5: Key Generation for the cloud user

Number of cloud user should be intimated in beginning stage before outsourcing the data. Key will be generated for the N number of cloud user who is registered or initiated in cloud. Key generation is the method of generating keys for cryptography. A key involved in encrypt and decrypt whatever data is being encrypted or decrypted. For each level or user key is generated. Consider if ten cloud users are initiated then ten levels are created in cloud server and each level may have a generated key for accessing the data. Each Cloud user can upload the desired patient data in cloud. User or Patient provided with the access function to perform operation.

VII. CONCLUSION AND FUTURE WORK

In this paper, the issue of outsourcing of data in cloud is addressed by the method of key generation for cloud user. Cloud computing, besides providing a maximized effectiveness of shared resources, also provides an easy way of storing and retrieving data. Personal Health Records (PHRs) are designed to maintain lifelong details of patients. Automated Patient Identifier and Patient Care System is designed to count hospitalized patients based on the concept of Current Procedure Terminology (CPT) manager. Cloud storage service is accessed through the cloud computer service, web service application programming interface or by a cloud storage gateway. The cloud based workspace is centralized providing easy functionality to share. The cloud environment can provide improvements in system efficiency & density. As a part of future work, we have planned to implement the uploading of encrypted medical data in cloud and in the process of creating individual cloudlets for preventing unauthorized user.

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.

[3] Richard Lenz, Manfred Reichert (2006) IT support for healthcare processes– Premises, challenges and perspectives, Elsevier.

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

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

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

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

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

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

[10] 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.

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

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

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

[14] 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.

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

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

[17] 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.

[18] 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.

[19] 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.

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

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

[22] 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

[23] 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.

[24] 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

[25] 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

[26] 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

[27] 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.**