Entity Relationship Looming of Efficient Protection Strategies to Preserve Privacy of Personal Health Records (PHRs) in Cloud

V.M.Prabhakaran¹, Prof.S.Balamurugan², S.Charanyaa³
PG Scholar, Department of CSE, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India¹
Assistant Professor, Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India²
Senior Software Engineer Mainframe Technologies Former, Larsen & Tubro (L&T) Infotech, Chennai, TamilNadu, India³

ABSTRACT: This paper proposes various entity relationship models to efficiently guard Electronic Health Records (EHRs). Privacy-An important factor need to be considered while we publishing the microdata. Usually government agencies and other organization used to publish the microdata. On releasing the microdata, the sensitive information of the individuals are being disclosed. This constitutes a major problem in the government and organizational sector for releasing the microdata. In order to sector or to prevent the sensitive information, we are going to implement certain algorithms and methods. Normally there two types of information disclosures they are: Identity disclosure and Attribute disclosure. Identity disclosure occurs when an individual's linked to a particular record in the released Attribute disclosure occurs when new information about some individuals are revealed. This paper aims to discuss the existing techniques present in literature for preserving, incremental development ER model of the system proposed.

KEYWORDS: Electronic Health Records(EHRs), Privacy, Microdata, Medical Healthcare System, Database Security.

I. INTRODUCTION

Cloud computing is new paradigm for distributed computing which delivers Infrastructure AS A Service (IaaS), Platform as a Service (PaaS), and Software as a Service(SaaS) and are made available as subscription-based services in a pay-as-you-go model to consumers computing on to the cloud SurajPandey, LinlinWu, Siddeswara Guru, RajkumarBuyya [2010]. It aids customers to dynamically provision computing resources around the globe, and also a. In order to efficiently and cost effectively schedule the tasks and data of applications onto these cloud computing environments, application schedulers have different policies that vary according to the objective function: minimize total execution time Rami.J.Matarneh [2009], minimize total cost to execute, balance the load on resources used while meeting the deadline constraints of the application, and so forth. In this paper, we focus on minimizing the average waiting time of tasks waiting for resources.

The need for efficient CPU allocation turns out to be the most important factor in today’s operating systems. Especially with the advent of multitasking environment, the allocation of CPU to a task requires more careful attention, than in a uni-task, uni-user architecture. A good scheduling algorithm would assure unbiased fairness as well as prevent starvation or stagnation of task. Need for an efficient scheduling mechanism in a multi programmed environment is very high, since the implementation of an operating system is itself, through one or more tasks. The need for multitasking is high. Also the need to complete the interrupt or any of the I/O operation within a stipulated time is very high. Designing a novel task scheduling algorithm should be governed by the following operational criteria of maximizing the CPU utilization and throughput and minimizing the turnaround time, waiting time and response time Abraham Silberschatz, Peter Baer Galvin and Greg Gagne [2005].
The remainder of the paper is organized as follows. Section 2 deals about Survey of Literature of Techniques prevailing to protect EHRs. Architectural representation of the proposed system is discussed in Section 3. Section 4 discusses about the existing and proposed techniques for securing PHR. The Sequence Flow Modeling of Key Generation is discussed in Section 5. Section 6 discusses about Sequence Flow Modeling of Data Uploading Process. The Sequence Flow Modeling of Data Retrieval Process is depicted in Section 7. Section 8 discusses the Sequence Flow Modeling of Data Sharing Process. Section 9 concludes the paper and outlines the direction for Future Work.

II. LITERATURE SURVEY

Workflow applications are commonly represented as a directed acyclic graph. The mapping of jobs to the compute-resources is an NP-complete problem as mentioned by J.D.Ullman (1975). The author proved that the problem of finding an optimal schedule for a set of jobs is NP-complete. The mapping of tasks to compute-resources is an NP-complete problem in the general form. The problem is NP-complete even in two simple cases: (in the negative a conjecture of R. L. Graham, Proc. SJCC, 1972, pp. 205-218).

(1) Scheduling tasks with uniform weights to an arbitrary number of processors and
(2) Scheduling tasks with weights equal to one or two units to two processors

As a consequence, the general preemptive scheduling problem is also NP-complete.

Scheduling is the key to the performance of grid workflow applications. Various strategies are proposed, including static scheduling strategies which map jobs to resources before execution time, or dynamic alternatives which schedule individual job only when it is ready to execute. While sizable work supports the claim that the static scheduling performs better for workflow applications than the dynamic one, it is questioned how a static schedule works effectively in a grid environment which changes constantly. Zhifeng Yu and Weisong Shi (2007) proposed a novel adaptive rescheduling concept, which allows the workflow planner works collaboratively with the run time executor and reschedule in a proactive way had the grid environment changes significantly. An HEFT-based (Heterogeneous Earliest Finish Time) adaptive rescheduling algorithm is presented, evaluated and compared with traditional static and dynamic strategies respectively. Executor will notify the planner of any run time event which interests the planner, for example, resource unavailability or discovery of new resource. Planner responds to the event by means of evaluating the event and rescheduling the remaining jobs in the workflow if necessary. The experiment results showed that the proposed strategy not only outperforms the dynamic one but also improves over the traditional static one. It is also observed that the proposed strategy performs more efficiently with data intensive application of higher degree of parallelism. The standard particle optimization algorithm generally is used to solve continuous optimization problems, and is used rarely to solve discrete problems such as JSSP (Job Shop Scheduling Problem). Z. Lian, B. Jiao, and X. Gu (2006) presented a similar PSO algorithm to solve JSSP. The job-shop scheduling problem (JSSP) is a branch of production scheduling, and it is well known that this problem is NP-hard. Many different approaches have been applied to JSSP and a rich harvest has been obtained. However, some JSSP, even with moderate size, cannot be solved to guarantee optimality Three representative (Taillard) instances were made by computational experiments, through comparing the SPSO algorithm with standard GA, and authors obtained that the SPSSOA is more clearly efficacious than standard GA for JSSP to minimize make span.

PekkaRuotsalainen (2004) [24] in “A cross-platform model for secure Electronic Health Record communication”. Enhanced cross security platform is proposed which support a platform for communication through the adhoc network to access the distributed electronic health records. Roger J. Quy (2005) [25] in “Method and apparatus for health and disease management combining patient data monitoring with wireless internet connectivity”. The health related data is communicated from the WWD to a server using standard internet protocols. Server calculates the response time and further it reviewed by a physician or health care provider. User and server interaction takes place the server transmits a response to the WWD and the user may answer the response.

Avner Amir, Avner Man (2006 a) [26] in “System and method for administration of on-line healthcare”. The end-unit device is guided by the CMIP so that anamnesis, diagnosis treatment is provided, monitored, recorded and clinically investigated. This system is useful for the management of medical records. Paul C. Tang, Joan S. Ash, David W. Bates,
J. Marc overhage and Daniel Z. Sands (2006 b) presented “Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption” they explore the Personal Health record (PHR) systems for patients. They carry patient data, they combine data, knowledge and software tools which help the patient to handle their medical data they handle through a standalone computer.

Christopher Alban, KhiangSeow (2007) [28] defines a “Clinical documentation system for use by multiple caregivers” they explain that A computer based system for recording, storing, accessing and retrieving clinical documentation where the care setting is provided. In a single electronic database it stores clinical patient notes, provides multiple points of read/write access through user interface operating on single or more client computers that are in real time communication with the repository.

III. ARCHITECTURAL REPRESENTATION

System has a Network model for the cloud data storage. It has several entities such as Data owner, Cloud storage, Cloud service provider and user. The Data owner encodes some keywords about the report or data, and service provider sustained the owner to reclaim the data by keywords and protect from the unauthorized persons. Cloud service provider is managed by the cloud server.

![System Architecture Diagram]

User is an object which has outsized data files to be stored and analyzed effectively in the cloud server and relies on the cloud for data maintenance and computation. User can be either individual clients or organizations. Legal permissions are provided to those who process and the request condition with the cloud server and get the grant permission to functionalize the process. User has functionality to

- Upload
- Retrieve
- Share
Revocation
Download

System uses the specialized algorithm AES (Advance Encryption Standard). It is based on a design standard known as a substitution permutation system which has the combination of both substitution and permutation functions and it is fast in both software and hardware process compare to its predecessor DES (Data Encryption Standard).

IV. ER-DIAGRAM FOR PHR SYSTEM

Interaction representation for PHR System has several entities such as PHR, Patient, Registration, Hospital, Tests, Identities, Reports and Treatment. Each entity has several attributes with the relationship in a flow manner. Hospital or Institution contains the In-patient medical module which contains the Patient ID, Patient name and membership date on which the treatment process has been started. They process various tests for several diseases and surgical problems and provide the prescription and drugs which need to be console.

Patient or user details are been registered in PHR it contains information such as Name, Date of birth, Age, Gender, Address, Contact number, Email address and Blood group. PHR also stores several Identities such as Height, Weight, personal identification and other problems. A feasible and promising approach would be to encrypt the data before outsourcing. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users.

V. ER-DIAGRAM FOR USER PROCESS

Interaction representation for User has several entities and relationship such as user, Legal and Illegal user, Tasks, Functions, Initiate, Upload, Retrieve and Share. User may be Legal and Illegal user. Legal user is the one who has the authorized permission to process all the functions in the PHR system. Legal user first process is to initiate the levels, once the level of user is defined by the data owner. It has several groups and once defined they log in and get the assigned key for encryption and decryption process.
Second process is the Upload function any level of user can access the cloud. The data which is being monitored and analyzed by the data owner such as doctor or institution involved in outsourcing the patient report. It helps the patient to access the health record details at any place at any time. After uploading the data it’s been encrypted to prevent from the threats. Next process is to extract or retrieve the outsourced data. User can view and analyses the health data. Only authorized person can access the data, unauthorized user doesn’t have permission to access the file or data which is been outsourced. Main benefits in Retrieval process is it does not need any conversion tool to view and analyses the data. Final function share process which involve in sharing of health data to the care provider or institution. Once stored in MYPHR machine patient can share who have been originated in cloud and the authorized permission is given.

VI. **ER-DIAGRAM FOR DATA OWNER PROCESS**

Data owner may be the Institution or organization who is the head of the process in MYPHR machine. Data owner has several entities and attributes such as Access, Store, Revocation, Provide permission, updation, rework, check user, authenticated, connection, user details, file and file size.
Permission is provided however, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patient’s control over access to their own PHRs it is a promising method to encrypt the PHRs before outsourcing. Also focus on addressing the complicated and challenging key management issues. In PHR framework it handles simultaneously different types of PHR sharing applications requirements, while incurring minimal key management overhead for both owners and users in the system. Revocation involves in swapping the user data with the new updated file and rework functions. Finally when we finished all the process it changes the generated key and log off, so we can prevent from the unauthorized parities.

VII. ER DIAGRAM FOR CLOUD SERVER

Cloud server has several entities and attributes in MYPHR machine such as Generate key, File handling, group level, store data, encrypt file, specify file size, data owner permission, issue different keys, revocation and conversion. MCloud Storage Server (CSS) is an object which is managed by Cloud Service Provider (CSP) has significant storage space and computation resource to maintain the user data. Data owner permission is essential to generate the key and issue different keys for every level or user who have been initiated. Files are been handled, stored and encrypted. Revocation is done in final stage of the process when all the authority function gets over.
VIII. 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 design the UML diagrams to look into the problem and to increase the clarity and to implement the uploading of encrypted medical data in cloud and in the process of creating individual cloudlets for preventing unauthorized user.

REFERENCES

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

[16] Edwin C. Bif 1997, Computerized medical diagnostic system including re-enter function and sensitivity factors, US5594638 A.
[23] Jeffrey J. Clawson 2003, Method and system for an improved entry process of an emergency medical dispatch system
[34] J. Vidhyalakshmi, J. Prassanna 2012 b, Providing a trustable healthcare cloud using an enhanced accountability framework.
[37] Abhishek Kumar Gupta, Kulvinder Singh Mann 2014 b, Medical Information on Cloud Platform.
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

BIOGRAPHY

V.M.Prabahakaran 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 Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. He has to his credit 22 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, Kalaignar Karunanidhi Institute of Technology. He has secured a best paper award in an International Conference held at Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, 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 65 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, Tamil Nadu, India. He is State Rank holder in school. 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 16 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. He is the author of 3 books titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7, "Principles of Scheduling in Cloud Computing" ISBN: 978-3-639-66950-3, and "Principles of Database Security", ISBN: 978-3-639-76030-9.

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 27 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, Amsterdam 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 3 books titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7, "Principles of Scheduling in Cloud Computing" ISBN: 978-3-639-66950-3, and "Principles of Database Security", ISBN: 978-3-639-76030-9.