**HEART RATE VARIABILITY AND PERSONAL HEALTH RECORDS MONITORING SYSTEM**

*Mr.T. Saransujai 1, G.S. Rizwana Banu 2,*

*V. Dharanidharan 3, K. Keerthana 4, S. Keerthana 5 and M. Meena 6*

*Assistant Professor 3, 4, 5, UG scholar 3,4 ,5*

*Department of Computer science and Engineering, K.S.R College of Engineering, Tiruchengode , Namakkal*

*Email id: kumarankay@yahoo.com 1, gsrizwana@gmail.com2, dharanidharan.v1413018@ksrce.ac.in3, keerthana.kcse@ksrce.ac.in4,* [*keerthana.s1413047@ksrce.ac.in5*](mailto:keerthana.s1413047@ksrce.ac.in5)*,* [*meena.mcse@ksrce.ac.in6*](mailto:meena.mcse@ksrce.ac.in6)*.*

**Abstract:** *Within Internet of Things (IoT) trend, there are intelligent devices that have a digital entity and are ubiquitously interconnected on a network and to the global Internet. IoT is mainly concentrated on providing user with the services to access the Internet-enabled electronic devices. These devices will collect data from the device and send it to the server. The server will further analysis on the data sent by the server and predict the results.The project deals with the hospital branch and patients management. Since cloud computing delivers convenient, on-demand access to shared pools of data, applications and hardware over the internet, it provides unlimited infrastructure to store and execute patient data and program. Due to this redundancy the data can be easily modified by unauthorized users which can be stored in the database. This leads to loss of data privacy and security to database. The proposed scheme ensures that cyclic redundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprise environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc.*

**I INTRODUCTION**

**PROJECT DESCRIPTION**

The project deals with the hospital branch and patients management. Since cloud computing delivers convenient, on-demand access to shared pools of data, applications and hardware over the internet, it provides unlimited infrastructure to store and execute patient data and program.

Due to this redundancy the data can be easily modified by unauthorized users which can be stored in the database. This leads to loss of data privacy and security to database.

The proposed scheme ensures that cyclic redundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprise environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc.

The testing application to enable Data Storage Security in Cloud Computing for Hospital Enterprises designed using Microsoft Visual Studio .Net 2005 as front end.

The coding language used is Visual C# .Net. The web technology used is ASP .Net 2005. MS-SQL Server 2000 is used as back end database.

**PERSONAL HEALTH CARE RECORD**

The earliest mention of the “personal health record” term was in an article indexed by PubMed dated June 1978, and even earlier in 1956 reference is made to a personal health log. Most scientific articles written about PHRs have been published since 2000.

“PHR" has been applied to both paper-based and computerized systems; current usage usually implies an electronic application used to collect and store health data. Several formal definitions of the term have been proposed by various organizations in recent years.

PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR.

PHRs can contain a diverse range of data, including but not limited to:

1. imaging reports (e.g. X-ray)
2. laboratory test results
3. medications and dosing
4. allergies and adverse drug reactions
5. chronic diseases
6. illnesses and hospitalizations
7. prescription record
8. surgeries and other procedures
9. vaccinations and Observations of Daily Living (ODLs)

**OBJECTIVES**

The following are the objectives of the project

1. To encipher the message that cannot be deciphered by malicious attackers.
2. To apply the TripleDES (Data Encryption Standard) algorithms in encrypting and decrypting the content.
3. To increase the security in communicating the messages.
4. To maintain the patients information in cloud storage space.
5. To maintain the visits, prescription and receipt details in cloud storage space.

**2 LITERATURE SURVEY**

**SECURING PERSONAL HEALTH RECORDS IN CLOUD COMPUTING: PATIENT-CENTRIC AND FINE-GRAINED DATA ACCESS CONTROL IN MULTI-OWNER SETTINGS**

In the paper, they proposed a novel framework for access control to PHRs within cloud computing environment. To enable ﬁne-grained and scalable access control for PHRs, they leveraged attribute based encryption (ABE) techniques to encrypt each patients’ PHR data. To reduce the key distribution complexity, they divided the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Their proposed scheme is also ﬂexible, in that it supports eﬃcient and on demand revocation of user access rights, and break-glass access under emergency scenarios.

The main concern is about the privacy of patients’ personal health data and who could gain access to the PHRs when they are stored in a cloud server. Since patients lose physical control to their own personal health data, directly placing those sensitive data under the control of the servers cannot provide strong privacy assurance at all. First, the PHR data could be leaked if an insider in the cloud provider’s organization misbehaves, due to the high value of the sensitive personal health information (PHI).

**AUTHORIZED PRIVATE KEYWORD SEARCH OVER ENCRYPTED PERSONAL HEALTH RECORDS IN CLOUD COMPUTING**

This paper formulates and addressed the problem of authorized private keyword searches (APKS) on encrypted PHR in cloud computing environments. It ﬁrst presented a scalable and ﬁne-grained authorization framework for searching on encrypted PHR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable with the user scale of the system.

Then they proposed two novel solutions for APKS based on a recent cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efﬁciency and the other with enhanced query privacy. In addition to document privacy and query privacy, other salient features of their schemes include: efﬁciently support multi-dimensional, multiple keyword searches with simple range query, allow delegation and revocation of search capabilities. They implemented their scheme on a modern workstation, and experimental results demonstrate its suitability for practical usage.

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. It had never been easier than now for one to create and manage her own personal health information (PHI) in one place, and share those information with others. It enables a patient to merge potentially separate health records from multiple geographically dispersed health providers into one centralized proﬁle over passages of time.

### II EXISTING SYSTEM

The previous system there is no facility for the patient and the doctor to communicate the details about the prescription that doctor prescribe in the last visit. The patient has to maintain it manually as the personal record with him or some time it is maintained in the excel sheet or the Microsoft word this data can be viewed by any person. This sometime leads to the series problem for the patient and the doctor to check for the treatment and health details. The doctor has to think the prescription what he gave earlier for the specific person.

**1. DRAW BACKS OF THE EXISTING SYSTEM**

1. It is so difficult for the doctors to maintain the details of the patient and the prescription they suggest earlier.
2. More number of records is to be maintained.
3. The old record is to be destroyed if the space not exists.
4. Sometime long time record is to be maintained.
5. If it is maintained in excel or as the word document it can be viewed by any person if it maintained secretly it not possible.
6. Only Classification is carried out.

### III PROPOSED SYSTEM

The proposed system in which the doctor can easily track the patient health condition based on their HRV value. The HRV value is taken into two phases. One is classification, which is useful for the doctor to classify the patients and provide the appropriate treatment. The entire records about the patient will be encrypted and stored in the database for the feature reference. If the data about the patient is try to access by the other user the details will be in the form of the encryption.

The doctor want to open he has the facility to view the prescription without the encryption. The proposed system is required to eliminate the risk in unavailability of one branch information in other branch. The proposed system is using an approach such that with the cloud storage space, the hardware and software maintenance risk is reduced.

**1 PROFILE CONSTRUCTION**

**USER**

An entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers.

**CLOUD SERVER (CS)**

An entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure- correcting code to further tolerate faults or server crash as user’s data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data.

**ENSURING CLOUD DATA STORAGE**

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or mirror problem.

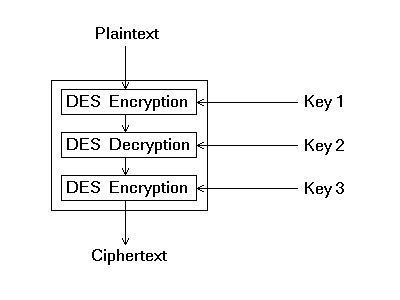
Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks.

To address these problems, the main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in this scheme for file distribution across cloud servers. Subsequently, it is shown how to derive a challenge- response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure- correcting code is also outlined. Finally, it describe how to extend the scheme to third party auditing with only slight modification of the main design.

**TRIPLE DES ENCRYPTION**

It is three times slower than regular DES but can be billions of times more secure if used properly. Triple DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days. No sane security expert would consider using DES to protect data.

Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end the National Institute of Standards and Technology (NIST) is holding a competition to develop the Advanced Encryption Standard (AES) as a replacement for DES. Triple DES has been endorsed by NIST as a temporary standard to be used until the AES is finished sometime in 2001.



**ADVANCED ENCRYPTION STANDARD**

AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files. Using a powerful 256-bit encryption algorithm, AES Crypt can safely secure the most sensitive files. Once a file is encrypted, user does not have to worry about a person reading the sensitive information, as an encrypted file is completely useless without the password. It simply cannot be read.

**DES( Data Encryption Standard)**

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers.

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message.

DES is the archetypal block cipher - an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such.

**ATTRIBUTE BASED ENCRYPTION**

The main goal of the framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) according to the different users’ data access requirements. The users who make access based on their professional roles, such as administrator, patients as users, and cloud provider. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government, or insurance sector.

For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

**ERROR RECOVERY ALGORITHM**

Error localization is a key prerequisite for eliminating errors in storage systems. It is also of critical importance to identify potential threats from mirror problem. The scheme outperforms those by integrating the correctness verification and error localization. The user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that the verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one.

**4**. **ADVANTAGES OF PROPOSED SYSTEM**

1. The data maintained in the system it is easy for the picking of patient details.
2. The data will be in the encrypted form.
3. Less number of time is required for the storing the details of the patient.
4. The next visit details can also viewed correctly.
5. The record is maintained safely.
6. The data can be fetched anywhere where we need the data.
7. Classification and Clustering is performed.

**IV CONCLUSION**

It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the project is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The project effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

**References**

1. Z. Dou, R. Song, and J.-R. Wen, “A Large-Scale Evaluation and Analysis of Personalized Search Strategies,” Proc. Int’l Conf. World Wide Web (WWW), pp. 581-590, 2007.
2. R. Krovetz and W. B. Croft. Lexical ambiguity and information retrieval. Information Systems, 10(2):115–141, 1992.
3. X. Shen, B. Tan, and C. Zhai. Implicit user modeling for personalized search. In Proceedings of CIKM ’05, pages 824–831, 2005.
4. J. Teevan, S. T. Dumais, and E. Horvitz. Beyond the commons: Investigating the value of personalizing web search. In Proceedings of PIA ’05, 2005.
5. X. Shen, B. Tan, and C. Zhai. Context-sensitive information retrieval using implicit feedback. In Proceedings of SIGIR ’05, pages 43–50, 2005.
6. M. Spertta and S. Gach, “Personalizing Search Based on User Search Histories,” Proc. IEEE/WIC/ACM Int’l Conf. Web Intelligence (WI), 2005.
7. OnStat. Most people use 2 word phrases in search engines according to onestat.com, February 2004. <http://www.onstat.com>.
8. Seruku. Seruku toolbar, 2004. <http://www.seruku.com/index.html>.
9. Mike Giles. Furl, 2003. <http://www.furl.net>.
10. B. Tan, X. Shen, and C. Zhai, “Mining Long-Term Search History to Improve Search Accuracy,” Proc. ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (KDD), 2006.
11. J. Allan et al. Challenges in information retrieval. In SIGIR Forum, volume 37, 2003.
12. T. Joachims. Optimizing search engines using clickthrough data. In Proceedings of SIGKDD 2002, pages 133–142, 2002.
13. X. Shen, B. Tan, and C. Zhai. Ucair toolbar: A personalized search toolbar (demo). In Proceedings of SIGIR 2005, page 681, 2005.
14. X. Shen, B. Tan, and C. Zhai. Context-sensitive information retrieval using implicit feedback. In Proceedings of SIGIR 2005, pages 43–50, 2005.
15. K. Sugiyama, K. Hatano, and M. Yoshikawa, “Adaptive Web Search Based on User Profile Constructed without any Effort from Users,” Proc. 13th Int’l Conf. World Wide Web (WWW), 2004.
16. R. Cooley, B. Mobasher, and J. Srivastava. Data Preparation for Mining World Wide Web Browsing Patterns. Knowledge and Information Systems, 1(1):5–32, 1999