International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 5, Sep – Oct 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

PREVENTING MIRROR PROBLEM AND PRIVACY ISSUES IN MULTISTORAGE AREA WITH DIMENSIONALITY REDUCTION

R.Mahendran[1], C.Karthik[2], M.Jothimani[3], K.P.Uvarajan[4]

Assistant Professor, ECE, K.S.R. College of Engineering, Tiruchengode[1,2,3,4]

rmahendranme@gmail.com[1],rpckarthikraja@gmail.com[2],mjothimanibe@gmail.com[3],uvaraj.kp@gmail.com[4]

Abstract:

In previous research of privacy issues in data storage is usually a patient to create, and control the personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information efficiently. Each patient is promised the full control of the medical records and can share the health data with a wide range of users, including family members, friends or healthcare providers. 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 patients control over access to their own Personal Health Records (PHR), this method encrypts the PHR before given to third parties. This paper proposes a novel patient-centric framework and also mechanisms for data access control to records stored in semi-trusted servers. To achieve scalable data access control for records, Encryption techniques are introduced to encrypt each patient's PHR data. Different from previous works in secure data outsourcing, it is now focused on the multiple cloud mirror scenario, and adopt different security mechanism such as different encryption methods in each attributes with the capability of the cloud software architecture.

Keywords: Privacy, Personal Health Records, Encryption, Cloud.

I. INTRODUCTION

The cloud is a familiar cliché is a metaphor for the Internet, but when combined with computing, the meaning gets bigger and fuzzier. Some analysts and vendors define cloud computing narrowly as an updated version of utility computing, basically virtual servers available over the Internet. Others go very broad, arguing anything users consume outside the firewall is in the cloud, including conventional outsourcing.

Cloud computing [1] comes into focus only when we think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. InfoWorld talked to dozens of vendors, analysts, and IT customers to tease out the various components of cloud computing. Based on those discussions, here's a rough breakdown of what cloud computing is all about:

Software as a Service (SaaS)

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications are different from other applications in their scalability-which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand.

Platform as a Service (PaaS)

In the PaaS [2] models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and

complexity of buying and managing the underlying hardware and software layers.

The computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.

***Infrastructure as a Service** (IaaS)*

In the most basic cloud-service model, providers of IaaS offer computers – physical or virtual machines – and other resources. A hypervisor, such as OpenStack, Xen, Hyper-V runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers varying requirements. IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, Virtual Local Area Networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds. Recently, this paradigm has been extended towards sensing and actuation resources, aiming at providing virtual sensors and actuators as a service.

II. BACKGROUND

The existing system is maintaining all branch patient's information in hospitals storage space. More number of IT professionals is required to keep availability of data at all time. More number of hardware assets and their management cost is also more

The importance of ensuring the remote data integrity for hospitals has been highlighted by some research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers to peers.

Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. However, while providing efficient cross server storage verification and data availability insurance, these schemes are all focusing on static or archival data. As a result, their capabilities of handling dynamic data remains unclear, which inevitably limits their full applicability in cloud storage scenarios. The presented system classifying the data based on the clustering work with similar items. So the data classification is not accuracy. The data is classified based on approximate k-NN search in high-dimensional spaces and then processed in another manner of a data reorganization method.

The thesis 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. The convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information, especially when they are stored on a third-party server which people may not fully trust.

A PHR [3] system where there are multiple owners and users. The owners refer to patients who Frequently Used Notations have full control over their own PHR data, i.e., they can create, manage, and delete it. There is a central server belonging to the PHR service provider that stores all the owners PHRs. The users may come from various aspects, for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. 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.

III. PROPOSED DESIGN

A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage,

retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of their medical records and can share their health data with a wide range of users, including healthcare providers, family members or friends.

The dissertation is required to eliminate the risk in unavailability of one branch information in other branch. The thesis is using an approach such that with the cloud storage space, the hardware and software maintenance risk is reduced. Owing to the number of drawbacks evident in the earlier system, the concept is being developed to computerized which leads to effectiveness of the users and their activities.

This facility enables people to record information that will substantiate achievement towards their objectives and goes a long way to resolving the issue of forgotten information that is relevant to the review. Information can be recorded all the way and assists both admin and user to recall information that will assist in the review.

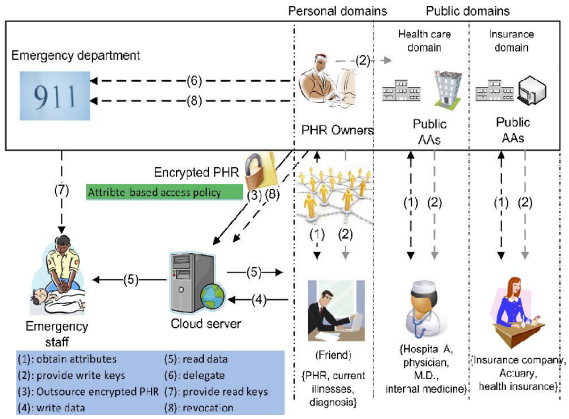

Figure 1 Proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multiowner settings.

The framework is illustrated in Figure 1. We term the users having read and write access as data readers and contributors, respectively. In our framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE [4] systems are involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, our proposed revocable MA-ABE scheme is used.

With distributed verification of erasure-coded data, the error recovery algorithm achieves the storage correctness insurance as well as data error localization. Whenever data corruption has been detected during the storage correctness verification, this scheme can almost guarantee the simultaneous localization of data errors.

In this thesis, to preferred implementation of k-NN search concept for classifying the patient record by Euclidean distance metric for analyzing the similar data based on one patient to another patient with the high dimensionality reduction technique.

IV. PREVENTING PRIVACY ISSUES BY DIFFERENT ENCRYPTIONS IN CLOUD AREA

A. 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 (PUD) and PerSonal Domains (PSD) according to the different user's 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, it 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.

B. Triple DES Encryption Standard

Triple Data Encryption Algorithm is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) [5] cipher algorithm three times to each data block. 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 and it breaks 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 AES as a replacement for DES.

The AES will be at least as strong as Triple DES and probably much faster. Many security systems will probably use both Triple DES and AES for at least the next five years. After that, AES may supplant Triple DES as the default algorithm on most systems, if it lives up to its expectations. But Triple DES will be kept around for compatibility reasons for many years after that. So the useful lifetime of Triple DES is far from over, even with the AES near completion. For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information.

Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, user simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL (Dynamic Link Library) then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. In figure 2, the data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

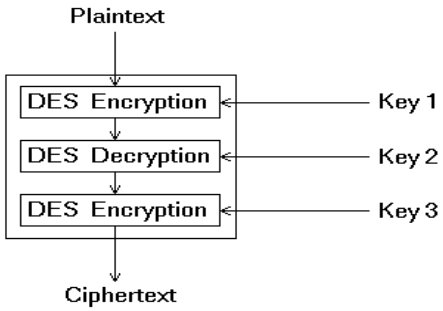

Figure 2 Structure of triple DES

Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Unfortunately, there are some weak keys that one should be aware of it. If all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES.

Note that although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1's in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

C. Advanced Encryption Standard

AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard 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.

AES Crypt is the perfect tool for anyone who carries sensitive information with them while traveling, uploads sensitive files to servers on the Internet, or wishes to protect sensitive information from being stolen from the home or office. AES Crypt is also the perfect solution for those who wish to backup information and store that data at a bank, in a cloud-based storage service, and any place where sensitive files might be accessible by someone else.

AES Crypt is completely free open source software. Since it is open source, several people have contributed to the software and have reviewed the software source code to ensure that it works properly to secure information.

D. Data Encryption Standard

Encryption is the process of converting a plaintext message into cipher text 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 cipher text 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.

E. 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.

F. K-Nearest Neighbor Search

k-NN is a non parametric lazy learning algorithm. When user say a technique is non parametric, it means that it does not make any assumptions on the underlying data distribution. This is pretty useful, as in the real world, most of the practical data does not obey the typical theoretical assumptions made.

Non parametric algorithms like k-NN come to the rescue here. It doesn't use the training data points to do any generalization. In other words, there is no explicit training phase or it is very minimal.

The training phase is pretty fast. Lack of generalization consumes that k-NN keeps all the training data. More exactly, all the training data is needed during the testing phase. This is in contrast to other techniques like Support Vector Machine (SVM) where it can discard all non support vectors without any problem.

Nearest Neighbor based Content Retrieval

This is one the fascinating application of k-NN. Basically user can use it in Computer Vision for many cases. It can consider handwriting detection as a rudimentary nearest neighbor problem. The problem becomes more fascinating if the content is a data given a data find the video closest to the query from the database.

If user wants to prepare a dictionary for American Sign Language (ASL) [6] so that user can query it doing a gesture. Now the problem reduces to find the possibly k closest gestures stored in the database and show to user

.

V. IMPLEMENTATION RESULTS

- The security of the proposed enhanced PHR sharing solution is implemented in the application and cloud area.
- The DES, Triple DES and AES algorithms in cloud environment, emphasizing possible improvements and vulnerabilities in implementation of cryptographic algorithms, usage of cryptographic frameworks and libraries, as well as the speed of execution of implemented cryptographic algorithms.
- Triple DES: It was enhancement of DES and used to remove the mid-in-the-middle attack occurred in 2-DES. In this 3 times iterations of DES encryption on each block is performed.
- In Triple-DES the 3-times iteration is applied to increase the encryption level and average time. Common method of Triple-DES is Minus Encrypt – Decrypt - Encrypt (-EDE). Each iteration of 3-DES using-EDE will encrypt a block using a 56-bit key.
- After encryption use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key.
- The algorithm is most popular and a symmetric key cryptographic algorithm. It may used to provide both secrecy and data authentication. It uses the prime number to generate the public and private key based on

mathematical fact and multiplying large numbers together.

The storage size of AES, DES and Triple DES algorithm is high in encrypting the data are different in length. Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput increased than power consumption decreased.

Table 1 evaluates the plain data size and encrypted data storage size in the tabular format and these results are represented in the chart format in the Figure 3. In this visit details, to process ten patients records along with patient identity number. Each patient record is differing from another patient. Here visit details are encrypted using DES encryption algorithm.

Patient Id	Source Size (In Bytes)	Encrypted Size (In Bytes)
1	68	212
2	82	232
3	104	272
4	110	252
5	60	212
6	74	212
7	112	272
8	91	252
9	120	272
10	141	316

Table 1 Visit Details

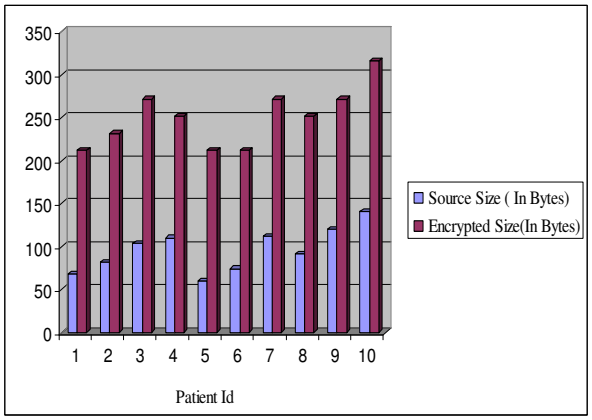

Figure 3 Chart representation for Visit Details

In the receipt details, the record should process in the application with the specification details such as branch id, patient Id, data of receipt, remarks, cheque number, consulted doctor name, visited branch name. This information's are encrypted using Triple DES algorithm and stored in the main server and multi cloud server at simultaneously. Table 2 is used to represent the receipt details of the patients and Figure 4 is used to represent the pictorial chart representation of the patients receipt details.

Patient Id	Source Size (In Bytes)	Encrypted Size(In Bytes)
1	68	140
2	91	164
3	114	196
4	86	164
5	132	216
6	66	144
7	92	184
8	50	120
9	66	144
10	101	184

Table 2 Receipt Details

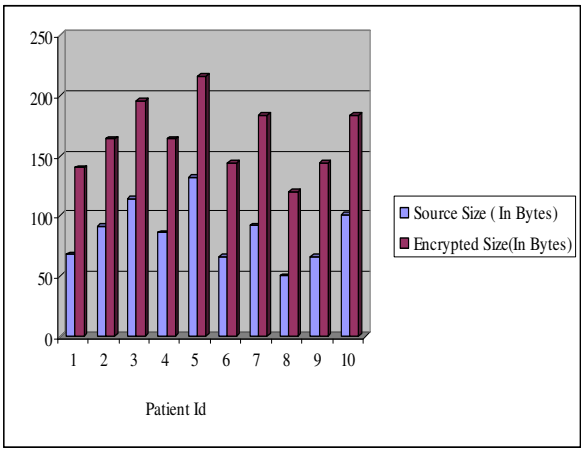

Figure 4 Chart representation of Receipt Details

In the Prescription details, the record should process in the application with the specification details such as branch id, patient Id, date, tablet name and with its quantity, charges of the tablet, remarks, consulted doctor name, visited branch name. This information's are encrypted using AES algorithm and stored in the main server and multi cloud server at simultaneously. Table 3 is used to represent the prescription details of the patients and Figure 5 is used to represent the pictorial chart representation of the patient's prescription details.

Patient Id	Source Size (In Bytes)	Encrypted Size(In Bytes)
1	63	232
2	76	232
3	92	272
4	74	232
5	131	316
6	103	276
7	77	232
8	66	232
9	79	252
10	116	276

Table 3 Prescription Details

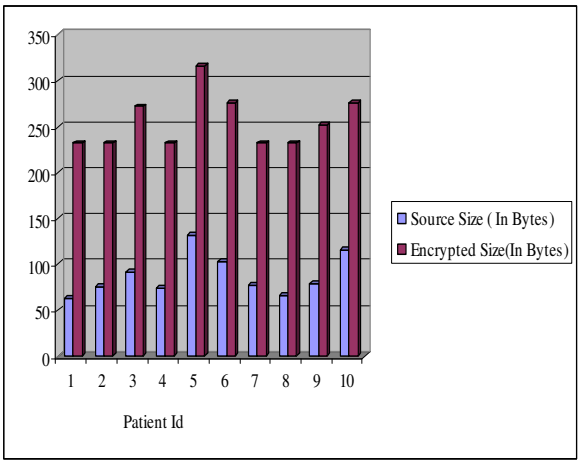

Figure 5 Chart representation of Prescription Details

VI. CONCLUSION

It is believed that almost all the system objectives that have been planned at the commencement of the software development and the implementation process of the dissertations are 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. In this thesis, it describes the design and prototype implementation of a social healthcare network over the cloud. The system is secured with a trust-aware attribute-based access control. The work addresses an unmet need in social healthcare networking -emotional support, and demonstrates social healthcare network application in a real cloud-computing environment.

REFERENCES

[1] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded, 2006. [Online]. Available:http://articles.latimes.com/2006/jun/26/health/he-privacy26

[2] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private, BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.

[3] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-

owner settings," in SecureComm'10, Sept. 2010, pp. 89-106.

[4] H. L ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud, in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[5] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing, in ICDCS '11, Jun. 2011.

[6] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing, in ICDCS '11, Jun. 2011.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records, in CCSW '09, 2009, pp. 103–114.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing, in IEEE INFOCOM'10, 2010.

