ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Design and Implementation of a Secure Healthcare Social Cloud System

[1]Mr. S.Sambasivam, MCA.,MPhil., Associate Professor,
[2]Mr. M.Selvam, Final MCA,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: sammy2173@gmail.com, selvamkgm007@gmail.com

***Abstract*—A patient-centric model of health information exchange is termed as personal health record (PHR). The service allows 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.**

It is also an emerging patient-centric method of health information exchange, which is often given to third parties, like cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

Index Terms- Personal Health Record (PHR), Personal Health Information (PHI), Electronic Health Records (EHRs), DES And AES Algorithms.

I. INTRODUCTION

Cloud computing is all the rage. "It's become the phrase du jour," says Gartner senior analyst Ben Pring, echoing many of his peers. The problem is that (as with Web 2.0) everyone seems to have a different definition.

"The cloud" is a familiar cliché s 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 you consume outside the firewall is "in the cloud," including conventional outsourcing.

Cloud computing comes into focus only when you 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.

At an early stage, cloud computing is with a motley crew of providers large and small delivering a slew of cloud-based services, from full-blown applications to storage services to spam filtering. Yes, utility-style infrastructure providers are part of the mix, but so are SaaS (software as a service) providers such as Salesforce.com. Today, for the most part, IT must plug into cloud-based services individually, but cloud computing aggregators and integrators are already emerging.

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:

A. 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.

B. *OBJECTIVES*:

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

II. RELATED WORKS

Shucheng Yu et al proposed "Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings" [1] the authors stated that online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data.

With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers.

Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.

Ahmad-Reza Sadeghi et al discussed about "Securing the E-Health Cloud" the authors stated that Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this context, the outsourcing of computation and storage resources to general IT providers (cloud computing) has become very appealing. E-health clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models.

However, they also bear new risks and raise challenges with respect to security and privacy aspects. In the paper, they pointed out several shortcomings of current e-health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-health systems.

To fill this gap, they presented security architecture for establishing privacy domains in e-health infrastructures. Their solution provides client platform security and appropriately combines this with network security concepts. Moreover, they discussed further open problems and research challenges on security, privacy and usability of e-health cloud systems. They discussed the general problems of e-health systems and provide a technical solution for the protection of privacy-sensitive data, which has not been appropriately addressed yet for end-user systems. In particular, their contributions are as follows:

They described an abstract model of e-health clouds, which comprehends the common entities of healthcare telematics infrastructures. Based on this model, they outlined three main problem areas for security and privacy, namely (i) data storage and processing, (ii) management of e-health infrastructures, and (iii) usability aspects of end-users.

Shucheng Yuy et al explained Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing the authors stated that recently, personal health record (PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place, such as a third-party cloud service provider.

Although this greatly facilitates the management and sharing of patients' personal health information (PHI), there have been serious privacy concerns about whether these service providers can be fully trusted in handling patients' sensitive PHI. To ensure patients' control over their own privacy, data encryption has been proposed as a promising solution.

However, key functionalities of a PHR service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form. Basically, users' queries should be performed in a privacy-preserving way that hides both the keywords in the queries and documents. More importantly, in order to prevent unnecessary exposure of patients' PHI from unlimited query capabilities, each user's query capability should be authorized and controlled in a fine-grained manner, which shall be achieved with a high level of system scalability.

Jonathan s. Walda et al developed a patient Web portal that features a patient-controlled electronic journal" to allow patients to interact with their physician's electronic medical record. Patients can view and respond to health reminders, critique electronic chart information maintained by their doctor's office, enter additional clinical information, and prepare information summaries before an office visit.

Creating shared information resources to support a collaborative care model required analysis of the business, architectural, and workflow requirements of the patient-controlled clinical portal and the physician-controlled electronic medical record system. In this paper they described the challenges in aligning the two systems and serving the different user groups.

Coupling the Patient Gateway system, serving over 8700 patients of 90 physicians as of September, 2003, with the Longitudinal Medical Record system, serving over 4000 physicians, has required a clear definition of user goals and workflow, well-defined inter-faces, and careful consideration of system assumptions to succeed.

Interest in electronic patient-physician communication1 and patients-as-contributors to their own medical record2 have accelerated as health care organizations focus their efforts to improve the quality and delivery of care with technology.

Shucheng Yu stated that Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners.

To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. They achieved this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. their proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that their proposed scheme is highly efficient and provably secures under existing security models.

Naranker Dulay et al presented Shared and Searchable Encrypted Data for Untrusted Servers" [10] the authors stated that current security mechanisms pose a risk for organizations that outsource their data management to untrusted servers. Encrypting and decrypting sensitive data at the client side is the normal approach in this situation but has high communication and computation overheads if only a subset of the data is required, for example, selecting records in a database table based on a keyword search. New cryptographic schemes have been proposed that support encrypted queries over encrypted data but all depend on a single set of secret keys, which implies single user access or sharing keys among multiple users, with key revocation requiring costly data re-encryption.

In the paper, they proposed an encryption scheme where each authorised user in the system has his own keys to encrypt and decrypt data. The scheme supports keyword search which enables the server to return only the encrypted data that satisfies an encrypted query without decrypting it. They provided two constructions of the scheme giving formal proofs of their security. They also reported on the results of a prototype implementation.

III. SYSTEM METHODOLOGY

A. 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.

B. 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.

In some cases, the user may need to perform block level operations on his data. The most general forms of these operations it are considering are block update, delete, insert and append. Note that in this dissertation to put more focus on the support of file-oriented cloud applications other than non-file application data, such as social networking data. In other words, the cloud data are considering is not expected to be rapidly changing in a relative short period.

As users no longer possess their data locally, it is of critical importance to ensure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance (to enforce cloud storage service-level agreement) of their stored data even without the existence of local copies. The point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

C. DESIGN GOALS

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, the main aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

- *Storage correctness:* To ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.
- *Fast localization of data error:* To effectively locate the malfunctioning server when data corruption has been detected.
- *Dynamic data support:* To maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
- *Dependability:* To enhance data availability mirror problem, malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors.
- *Lightweight:* To enable users to perform storage correctness checks with minimum overhead.

D. 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.

E. 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.

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, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, 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. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

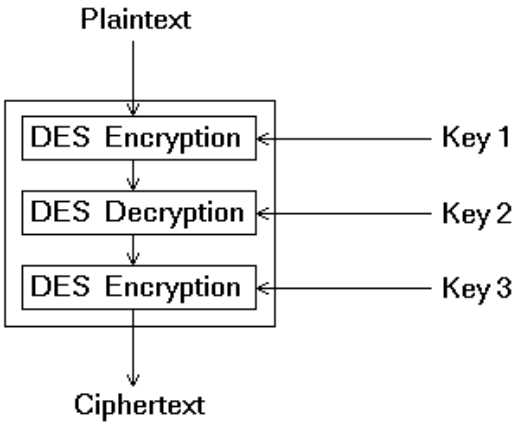

Fig1. DES Encryption

Consequently, 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: 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 1s 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.

F. 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.

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.

Best of all, 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. Most important to most users, though, is the fact that the software is available at no cost. To use this software in the business, at home, or in the own open source development projects.

G. 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.

H. 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.

I. 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.

Step 1: Start the process.
Step 2: Change the data at any one server in cloud area value as 0.
Step 3: Process the error recovery technique.
Step 4: Monitor and check the data in multiple cloud.
Step 5: Corrupted data will be displayed in the cloud area.
Step 6: Auto detection and correction work message will appeared in the application.
Step 7: Data change will be changed in the specified manner.

J. RESULT AND DISCUSSION

- The security of the proposed enhanced PHR sharing solution is implemented in the application and cloud area.
- It achieves data confidentiality (i.e., preventing unauthorized read accesses), by proving the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute-based selective-set model.
- The enhanced MA-ABE scheme guarantees data confidentiality of the PHR data against unauthorized users and the curious cloud service provider, while maintaining the collusion resistance against users.
- 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.

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.

V. FUTURE ENHANCEMENT

The following enhancements are should be in future.

- The application if developed as web services, then many applications can make use of the records.
- The next visit details can be sent as SMS to patients.
- The web site and database can be hosted in real cloud place during the implementation.

REFERENCES

[1] 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.

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

[3] 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.

[4] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5] "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

[6] "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

[7] 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.

[8] 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.

[9] 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.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[11] "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

[12] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 103–114.