Enhancement of Security in Cloud Storage of Electronic Health Records based on Secret Sharing

Mohith Gowda HR[1], Adithya MV[2]

[1]*B.E in Computer Science and Engineering, Mandya – 571401, Karnataka, India*
[2]*B.E in Computer Science and Engineering, Mandya – 571401, Karnataka, India*

Abstract - *Establishment of Security for Electronic Health Records (EHRs) has become an unresolved issue in the field of healthcare processing system. Among varies present trends in the field, the most effective method that provides flexibility, Economical is, the Cloud Storage Technology which provides Efficient way to store, manage and retrieve the electronic dataNevertheless, storing sensitive information such as health records on the cloud incurs severe security and privacy risks. This paper provides an effective and secure method to store EHRs in cloud using secret sharing and AES Algorithm. In this system, an EHR is divided into multiple segments by a healthcare centre, and the segments are distributed to numerous cloud servers. When retrieving the EHR, the healthcare centre captures segments from partial cloud servers and reconstructs the EHRs. Meanwhile, in reality, the reconstruction of a shared EHR could be much burdensome for a healthcare centre or a patient, we thus propose a practical cloud storage scheme which outsources the reconstruction of a shared EHR to a cloud computing service provider. Such a solution can drastically boost the efficiency of the proposed scheme, and the results of outsourcing reconstruction can be verified by healthcare centres or patients in our scheme. This system proposed and experimented has proven to provide better security and efficiency for EHRs.*

***Key Words*: AES Algorithm, Elliptic Curve Diffie-Hellman, Secure Cloud Computing, Symmetric Bivariate Polynomial Based Secret Sharing, Verifiable Reconstruction Outsourcing Based Secret Sharing.**

1. INTRODUCTION

The use of conventional health record system is dramatically decreasing, giving rise to the electronic health record system during the past few years. *EHRs* have many considerable advantages such as economy, normativity, efficiency and accessibility. This advanced system is beneficial to healthcare centre (HC) as well as the patients as the huge amount of data is stored and maintained in the cloud. cloud service provider offers rapid access to flexible, low-cost resources, thus benefitting the people to use these services in various fields including healthcare. With the development of large-scale, on-demand, flexible storing and computing infrastructures provided by cloud computing services, *HCs* could avoid the burden of data management, reduce the cost of storing massive data by themselves and achieve universal data access with location independence.

EHRs are usually private and confidential since they include patient identifiers and highly sensitive information. However, when using the cloud computing services, users do not have physical control over their data. And cloud service providers are not completely trusted , though the infrastructures under the cloud are much more reliable than personal computing devices. The ‘‘curious’’ clouds may have various incentives to be unfaithful toward the cloud users. They can either maliciously tamper the data or spy on some sensitive information. Therefore, cloud computing also brings security challenges while its advantages are appealing for *EHRs* storage.

There have been numerous approaches discussing data security and privacy protection issues in cloud computing environments. Encryption is a traditional method to protect the privacy of sensitive data stored in clouds. However, the storage of encryption key is a high-risk target and any negative incident may jeopardize all encrypted health records. Aiming to limit a single point failure problem, schemes based on secret sharing are proposed. Nonetheless, all the existing cloud storage solutions for *EHRs* based on secret sharing have some com- mon disadvantages: first, the management of encrypted key is too complicated; second, it is not practical for patients or *HCs* to execute the expensive reconstruction of shared *EHRs*. The encrypted key is an obvious and weak target for the whole actual implementation regardless of what symmetric or public-key encryption algorithm is employed. More- over, it demands tremendous time and resources of clients (patients or *HCs*) to perform the *EHR* reconstruction that involves time-consuming modular exponentiation operations, especially when a *HC* deal with enormous amount of *EHRs*. In order to avoid the complicated key management problem, we plan to pre-process the original *EHR* before its shares are stored in different clouds. Also, we tend to outsource the *EHR* reconstruction to a cloud computing provider to reduce the local computation burden.

It is our essential goal to propose a practical cloud storage solution for *EHRs* by using secret sharing to solve the single point failure problem. Unavoidably though, the reconstruc- tion of *EHR* can become a issue for personal or health- care hosts. As a response, we outsource the reconstruction operation to a cloud computing provider, which brings some other challenges. First, the cloud computing server might be curious on user's sensitive data, so we have to make sure that cloud computing server executing the reconstruction out- sourcing cannot obtain the original *EHRs*. Second, the cloud server might return incorrect results intentionally or unintentionally, so *HCs* have to be able to verify the correctness of the reconstructed *EHR*. Also, the recovery operation of the original *EHR* by client hosts should be simpler than the recon- structing operation. To address all the above challenges, we propose our cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing.

Our contribution can be summarized as follows:

1. We enhance a cloud storage system architecture for *EHRs* which employs the secret sharing and AES algorithm.
2. We propose a practical cloud storage scheme which satisfies the architecture. This system accounts reconstruction outsourcing technique in all cloud storage schemes for *EHRs* based on secret sharing, which can significantly improve the client side efficiency and security.

The rest of the paper is Structured as follows: in Section II, we conduct a literature review with their drawbacks. We illustrate the present system and the proposed model in Section III. In Section IV, we explain the modules of our secure cloud storage model. Finally, the conclusion is made in Section V.

2. LITERATURE REVIEW

[1] (F. Alsolami & T. E. Boult, 2104) have proposed the Cloud Stash scheme, a system that applied the secret-sharing scheme directly on the file to store multi-shares of a file into multi- clouds. Cloud Stash utilizes secret-sharing, low cost cloud storage s and multi-threading to improve confidentiality, availability, performance and fault tolerance. Cloud Stash achieves this improvement by splitting a file into multi- shares of secret and distributing these multi-shares into multi-clouds simultaneously where threshold shares are required to reconstruct the file. Their experiments show that Cloud Stash is significantly faster for small files, and even for large files the added cost is not statistically worse. So the added security benefits are nearly free from the users' perspective.

Disadvantages:

1. On larger files, the algorithms large variance in communication time results in the baseline is failing to be statistically significantly better.

[2] (M.J.Atallah, K.N.Pantazopoulos, J.R.Rice, & E.E. Spafford, 2002) have investigated the outsourcing of numerical and scientific computations using framework. A customer who needs computation to done lacks the computational resources, would use external agent to perform these computations. The outsourcing is secure if it is done without revealing to the external agent. In order to protect data, customer have to do some pre-processing and post-processing of data before sending and receiving respectively. So, they proposed a framework for disguising scientific computation. There is no single disguise technique to calculate accurate scientific computation but there is an array of disguise technique available so that almost any scientific computation could be disguised at a reasonable rate and with very high levels of security.

Disadvantages:

1. Complex in computation.
2. It requires huge time for small applications also.

[3] (X. Chen, J. Li, J. Ma, Q. Tang, & W. Lou, 2013) have proposed a new secure outsourcing algorithm for (variable-exponent, variable-base) exponentiation modulo a prime in the two untrusted program model. Authors claim that when compared with the state-of-the-art algorithm, the proposed algorithm is superior in both efficiency and check ability. Results demonstrate how to achieve outsource-secure Cramer-Shoup encryption s and Schnorr signatures. Another algorithm named first efficient outsource-secure algorithm is proposed for simultaneous modular exponentiation s. Finally, they report the experimental evaluation that demonstrates the efficiency and effectiveness of the proposed outsourcing algorithms and schemes.

Disadvantages:

1. Prevents collusion attack inside the cloud server.
2. Does not consider the access revocation.

[4] (R.D'Souza, D.Jao, I.Mironov, & O.Pandey, 2011) have constructed a new scheme based on pairings which is much more efficient than Stadler's scheme. Their scheme is non interactive and can support any monotone access structure. In addition, it is proven secure in the standard model under the Bilinear Diffie-Hellman (BDH) assumption. The PVSS scheme is the non-interactive scheme proven secure in the standard model; all previous non-interactive PVSS schemes assume the existence of a Random Oracle. The proposed scheme is simple, efficient and further their implementation demonstrates the scheme compares well with the current fastest known PVSS schemes.

Disadvantages:

1. There is no forward security and backward security.

[5] (T. Ermakova & B. Fabian, 2013) have evaluated and selected a secret-sharing algorithm for our multi-cloud architecture. They have implemented both Shamir's secret-sharing scheme and Rabin's information dispersal algorithm and performed several experiments measuring the execution time. Their results indicate that an adoption of Rabin's algorithm would create a low overhead, giving strong indicators to the feasibility of their approach.

Disadvantages:

1. In the case of key compromise, or if encryption algorithms are broken their implementation turns out to be insecure.

3. SYSTEM ANALYSIS

3.1 Existing System

Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Aiming to limit a single point failure problem, schemes based on secret sharing were proposed. Ermakova [5] proposed a scheme based on Shamir's (t, n) secret sharing which divided the encrypted EHRs into shares to be stored in different cloud service providers. This approach guaranteed that cloud service providers colluding to break the privacy cannot obtain EHRs, even if the encryption of EHRs is broken. Secret sharing is adopted in many cryptographic schemes in cloud computing environment. F. Alsolami [1] proposed a system named Cloud Stash, which applied the secret-sharing scheme directly on the file to store multi-shares of a file into multi-clouds. Compared with the traditional cloud storage, the proposed scheme achieved improvement on confidentiality, availability, performance and fault tolerance.

Disadvantages of Existing System:

1. The basic cryptographic operations are sometimes too expensive for resource-constrained devices.
2. Less secure.
3. Huge computation resources required to secure data.

3.2 Proposed System

In this section, we present our cloud storage scheme for EHRs based on secret sharing, which includes a novel concept-reconstruction outsourcing. The proposed cloud storage scheme for EHRs consists of four phases, namely the pre-processing phase, the distribution phase, the reconstruction outsourcing phase, and the recovery and verification phase. Before elaborating the proposed scheme, we first give the definition of reconstruction outsourcing. Reconstruction outsourcing is a processing method of reconstruction in a cloud storage solution based on secret sharing. Unlike a conventional way, the reconstruction of stored data in different cloud service providers is outsourced to a cloud computing provider, so that the computing resources of client hosts can be saved. In our case, the reconstruction outsourcing of pre-processed EHRs must make sure that the outsourcing cloud service provider cannot obtain any content of the EHRs during the reconstruction.

3.3 System Design

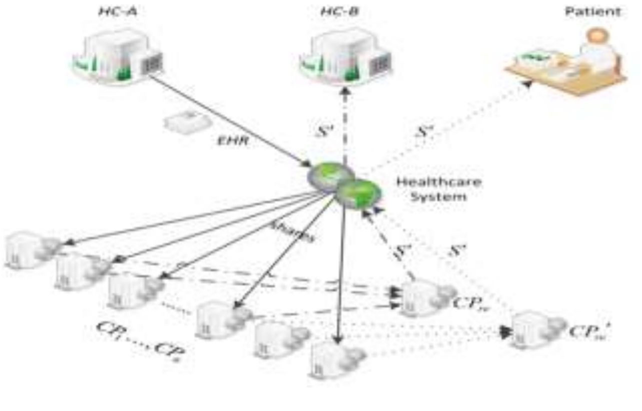

Fig- 1: Architecture of Cloud Storage System

Fig- *1* illustrates the system architecture. The system architecture is designed to store *EHRs* on different *HCs* using secret sharing. As shown in figure 1, the key components include: the pre-processing of *EHRs*, distribution of pre-processed *EHRs*, reconstruction outsourcing, verification and recovery of *EHRs*. We now describe the workflow of the system. Assuming that the *EHRs* are created by a healthcare centre named $HC - A$. After $HC - A$ uploads the *EHR* to a healthcare system, the healthcare system generates an unique identifier for it, which is relevant to patient's ID, $HC - A$'s ID, time stamp, etc. In the pre-processing phase, the healthcare system performs a bitwise exclusive OR operation between the *EHR* and its hash value. Then healthcare system dis- tributes the pre-processed *EHR* into n shares using Shamir's threshold secret sharing algorithm and sends the n shares to n different cloud service providers $CP_1,...,CP_n$ according the protocols between healthcare institutions and *CPs*. When the owner of the *EHR* or an authorized healthcare centre $HC - B$ wants to get the *EHR*, they send a request through the healthcare system. After confirming the request, health- care system assigns a cloud service provider CP_{re} (CP'_{re}) to do the reconstruction operation. The assigned outsourcing cloud service provider CP_{re} (CP'_{re}) gets t or more shares from $CP_1, \ldots, CP_n$. After finishing the reconstruction, CP_{re} (CP'_{re}) returns the result s' to $HC - B$ (or the patient) through healthcare system. At last, $HC - B$ (or the patient) can recover the original *EHR* with its hash value stored in healthcare system by simply performing a bitwise exclusive OR operation.

3.4 Sequence Diagram

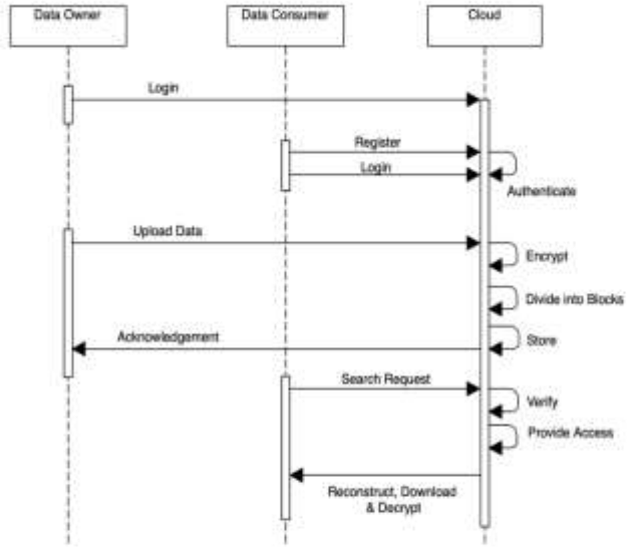

Fig- 2: Sequence Diagram for Owner and User Interaction

This system designed to store EHRs on different HCs using secret sharing is represented in the form of Sequence diagram as show in **Fig- 2**.

4. Methodology

4.1 Modules

A. Delegator Owner Module

In the owner module, Owner first login by patient Id. Owner uploads patient data. The authority delegation is realized mainly by proxy re-encryption mechanism. The proxy server makes use of the re-encryption key to transform the cipher text encrypted by owner's public key into another form, which can be searched by the user using his own private key.

B. User Module

In the User module, User like doctor, nurse login by their Id, Search for patient details and send the request to Owner. The delegate will be divested of the search authority when the effective time expires. In order to achieve the time-controlled access right revocation, the predefined time information is embedded in the re-encrypted cipher text with time seal. With the help of the time seal, the user is able to generate a valid delegation trapdoor by TrapdoorR algorithm. If the time information hidden in the re-encrypted cipher text is inconsistent with that in the delegation trapdoor, the equation in algorithm will not hold. The search query of the user will be rejected by the data server if the current time beyond the preset time.

C. Emergency

The Emergency will work based when patient is not in conscious emergency will send the request to take care to access the patient file. The Emergency will login by their Id's and send the request to caretaker of patient.

D. Time Controlled Revocation

An important design goal is to enable time-controlled access right revocation. The delegation appointment will terminate when the preset effective time period disagrees with the current time. It should prevent the authorized user from accessing the record's overtime.

E. AES Algorithm

- The Advance Encryption Standard (AES) is a symmetric-key algorithm for encryption of electronic data. It is highly influential in the advancement of modern cryptography.

- It consists of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
- In this project, we are using 128 bits of key for encryption and decryption.
- Steps involved for encryption of data:
    a) Byte Substitution
    b) Shift Rows
    c) Mix Column
    d) Add round key
- Same steps are required for decryption but in reverse order.

F. Shamir Secret Sharing Algorithm

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. Shamir's Secret Sharing is used to secure a secret in a distributed way, most often to secure other encryption keys. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part. To unlock the secret via Shamir's secret sharing, you need a minimum number of shares.

5. FINAL REMARKS

In this research, we proposed a privacy-preserving cloud storage scheme for electronic health records based on Shamir's Secret Sharing. To address the problem that the reconstruction of shared EHR is burdensome for a healthcare center or a patient in a real- world application, we proposed a secure outsourcing approach for the secret reconstruction of shared EHR. Through theoretical analysis, we demonstrated that our project satisfies the security requirements. As a conclusion, both the distribution phase and the reconstruction phase are time-consuming. This outsourcing approach effectively reduces the burden for the reconstruction phase. As for the distribution phase, since the user only needs to execute it once, we did not take it into concern when we design the scheme. Therefore, the outsourcing for distribution was not designed. As per now, we have gone through many papers, and we have observed that other paper lacks reconstruction of data, which make it less secure. As we know that, EHR is very sensitive data. So, we cannot take any risks regarding its security. This project can be further improved which can make it even more reliable in the future. The web pages will be constantly updated as data owner uploads the data of patients in cloud. Future development of user-friendly GUI, testing it on test users and finally publish the application on android which will be really helpful for hospitals.

REFERENCES

[1] F. Alsolami, & T. E. Boult. (2104). Cloudstash: Using secret sharing scheme to secure data, not keys, in multiclouds. Information Technology: New Generations (pp. 315-320). Las Vegas, NV, USA: IEEE.

[2] M.J.Atallah, K.N.Pantazopoulos, J.R.Rice, & E.E. Spafford. (2002). Secure outsourcing of scientific computations. Advances in Computers, 215-272.

[3] X. Chen, J. Li, J. Ma, Q. Tang, & W. Lou. (2013). New Algorithms for Secure Outsourcing of Modular Exponentiations. IEEE, 2386 - 2396.

[4] R.D'Souza, D.Jao, I.Mironov, & O.Pandey. (2011). Publicly Verifiable Secret Sharing for Cloud-Based Key Management. Progress in Cryptology – INDOCRYPT 2011 (pp. 290-309). Springer, Berlin, Heidelberg.

[5] T. Ermakova, & B. Fabian. (2013). Secret Sharing for Health Data in Multi-provider Clouds. Business Informatics (pp. 93–100). Vienna: IEEE.