International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT

ELSEVIER SSRN



IJIEMR Transactions, online available on 1st Jun 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-06

Title: EFFICIENT CLOUD STORAGE SYSTEM FOR HEALTH CARE RECORD MAINTENANCE USING SECRET SHARING TECHNIQUE

Volume 08, Issue 06, Pages: 252–258.

Paper Authors

**HARSHITHA H R, KEERTHANA S, MOUNIKA K, ROHINIT V**

SJB Institute of Technology, Bangalore,India


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# EFFICIENT CLOUD STORAGE SYSTEM FOR HEALTH CARE RECORD MAINTENANCE USING SECRET SHARING TECHNIQUE

[1]HARSHITHA H R, [2]KEERTHANA S, [3]MOUNIKA K, [4]ROHINIT V
[1,2,3]Dept. of ISE, SJB Institute of Technology, Bangalore,India
[4]Asst. Professor, Dept. of ISE,SJB Institute of Technology, Bangalore,India
harshi.ravi5@gmail.com, keerthana.shanthraj@gmail.com, mounikaramesh97@gmail.com, rohinitv@gmail.com

**Abstract**—now a days, storing massive amount of data in the cloud is an effective solution when compared to local storage due to its benefits like flexibility and scalability. This is being widely used in the health care systems (HCS) to store the Electronic health records (EHR). However, storing these sensitive information like EHR on the cloud induces severe security and privacy risks. In the proposed system, the security for the EHRs is given by Shamir's secret sharing technique and AES algorithm. The EHR will be fragmented and distributed to many cloud servers. The retrieval of these EHRs will include a reconstruction mechanism which will be outsourced to another cloud service provider to reduce the load for the HCS or patients.

**Keywords**—cloud computing,secret sharing,reconstruction,outsourcing

## I.INTRODUCTION

In the recent years, there is an extensive usage of EHRs in the HC systems over the regular health records due to its advantages such as economy, accessibility and efficiency. This electronic method provides a facile access to the data and increases the medical services. This type of storage should ensure that a huge amount of data can be saved and retrieved conveniently for every patient. The HCs could reduce the load of managing and maintaining the data by themselves by utilizing the services given by the cloud providers such as large scale, on-demand, flexible and computing infrastructures. By storing EHRs on the cloud the HCs can get universal access to the data with location independence. But while using cloud computing services the user will not have any physical control over the data, this imposes security challenges to the EHRs stored on the cloud. The EHRs have confidential information as it includes patient's identifier and other sensitive information. Therefore, an efficient technique to store EHRs securely on cloud should be used. Encryption being the typical method to ensure confidentiality for the EHR data, however, the storage of encryption keys become a challenge and increases the tendency of single point failure. In order to overcome this fault, secret sharing techniques are proposed. Yet, these schemes have their own demerits: firstly, management of encryption key is complicated. Secondly, it's not feasible for patients or HCs to carry out the

reconstruction process. In order to overcome the above-mentioneddemerits, the proposed system focuses on outsourcing reconstruction operation and preprocess the original EHR before its fragmentation. And the time based access control is incorporated to provide a specific time interval for the EHR access. This enhances the security of the system.The remaining part of the paper consists of the following sections: section II consists of the literature survey, section III briefs about the system's architecture, section IV consists of the implementation of the proposed scheme. The results of the proposed system and conclusion are given in section V and section VI respectively.

## II.RELATED WORK

The literature survey of the system includes referring the following papers.Zhang et al.[8] proposed a new system for securely storing medical health records using Shamir's secret sharing. It also emphasizes on outsourcing the reconstruction of thedistributed record to a cloud service provider thereby decreasing burden on the healthcarecenters or patients to do so.Even though there are numerous advantages of using cloud storage there is still security and key management issues. The cloud is prone to offline-brute-force attack, where the hacker can decrypt and obtain the key and use it offline. To overcome this problem, F. Alsolami et al[1]. proposed the Cloud Stash scheme where, multiple divisions of the file is stored in multi-clouds. Confidentiality, availability, performance and fault tolerance is improved by using Cloud Stash as it uses secret-sharing, low cost cloud storages and multi-threading.The involvement of an external agent to perform the computations necessary for the system could pose a threat of disclosing the actual data to this agent.Therefore, it is necessary toconceal the information before handing it over to the external agent.So, M.J.Atallah et al.[2] proposed a framework for this concealing mechanisms and discussed the security levels,their costs and numerical properties and thereby concluded that an array of techniques are available to carry out the data concealing at highsecurity and reasonable costs.However, the observation incurred huge time for small applications as well.Publicly Verifiable Secret-sharing (PVSS) schemes support the key-recovery functionsin a public cloud.R.D'Souza et al.[6] gave a holistic outlook for public key encryption.A more effective scheme compared to Stadler wasdeveloped based on pairings.This scheme was the pioneer non-interactive scheme to be proved in a standard model.However, the systemlacked forward and backward security.

T.Ermakova et al.[7] carried out a analysis with various German health expertsand obtained the requirements of establishing security of the medical data.The proposed architecture ensured additional security in situations like key compromise,disintegrated encryption algorithm implementations.Shamir's secret sharing and Rabin's information dispersal algorithm were used and Rabin's algorithm created a low overhead and sustainedthe workability of the given approach.

Chen et al.[5] proposed a reliable outsourcing algorithm for large-scale linear

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

equations.Thisneeded a single round interaction between the client and server and was efficient in finding out theirregularities of the cloud server with a probability 1.It is necessary to have an efficient method to outsource operations to untrusted cloud servers as exponentiations modulo a large prime is an expensive operation and it cannot be handled by resource-limited devices.So, X. Chen et .al[4] proposed a secure outsourcing algorithm to carry out the modular exponentiations parallelly. However, this system failed to consider the access revocation.

## III. SYSTEM ARCHITECTURE

Initially, the entities can register to the system by providing the necessary credentials. The admin performs the background verification of the registered users.The owner or the patient can upload the medical record to the cloud. The records will be preprocessed, segmented and distributed into n cloud providers. To overcome the security threats in cloud, the EHRs are encrypted using AES algorithm and then stored in the cloud. The new feature that is incorporated in our proposed scheme is the time based accessrights. The owner has the right to limit the access time given to the users to view the record, failing which the permission to view the records gets ceased despite the usershaving the necessary key credentials.Every user is given role based access rights, where the doctor has the right to view the full records and to edit the records, whereas, the nurse have only viewing rights.Whenever, a user requests for the EHR and when this request is passed by the owner, the CP which is meant for the reconstruction of the EHR will do so, which reduces the burden on the HC system and this is known as outsourcing. The retrieval process includes the requested user receiving the decrypted EHR from the cloud.During the emergency cases which leads to the unavailability of the EHR owner, the care taker will be in charge of processing the requests. The care taker can grant therequest only once in a day, which ensures that the security is not compromised in emergency situations.

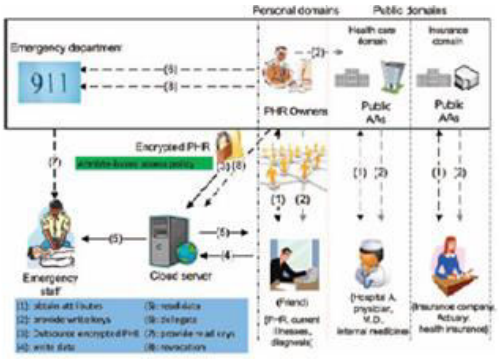


Fig 1: Overall architecture

The proposed system for EHR is implemented by using these four phases: pre-processing phase, distribution phase, reconstruction outsourcing phase, and the recoveryand verification phase.

1. Preprocessing

The HC system performs the preprocessing phase by uploading the EHR to the HC system. A unique identifier for the EHR and the hash valuefor the record, both are generated by the HC and stored at HC. The preprocessing of EHR is done by making every block of record do bitwise exclusive OR operation with hash value of the record. By using secret sharing technique, the preprocessed records will be segmented and distributed to n different cloud providers.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

2. Distribution

The distribution of preprocessed EHRs is done by the HC system. The n shares of the preprocessed records is determined by the HC system and allocated to CP1,CP2....CP n by the HC system itself, even the identifier will be uploaded to the CP by the HC system which can be used to extract the preprocessed EHRs.

3. Reconstruction Outsourcing

Evaluation of many linear equations is involved in reconstruction of a secret. Hence, it would be inconvenient for the HC system to perform reconstruction of EHRs. Therefore, the HC system outsources the reconstruction to a cloud serviceprovider, CP RE. CP RE might be a curious and a dishonest party,in such a case there a threat to the EHR. In order to avoid this, in the preprocessing phase, the original records is hidden by performing bitwise exclusive OR operation with the hash value of the record. Thus, security is provided to the EHR during reconstruction outsourcing process.

4. Recovery and Verification

The HC system receives the preprocessed records from the CP RE and takes the hash value from the HC system to recover the original records. Now, the HC system contains therecovered record and the original record. The HC performsverification processes to see if the recovered record is the same as the original record, otherwise the HC will recognizes that the EHR is not real.

A. FLOW CHART

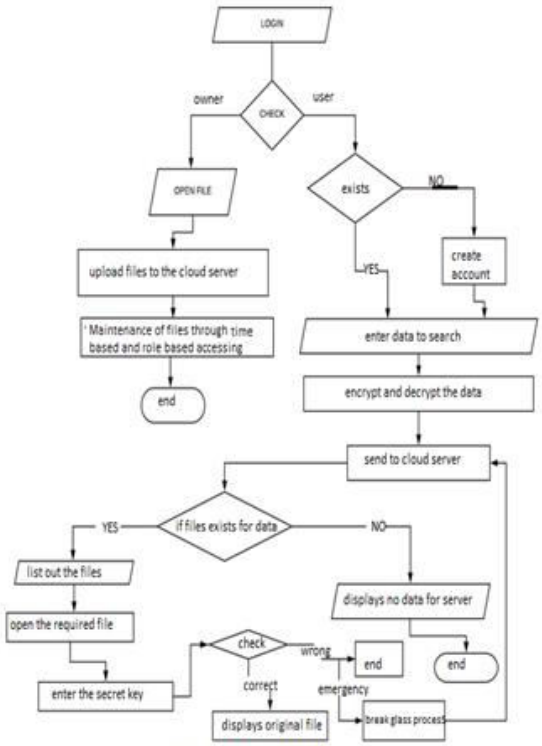


Fig 2: Flow chart

The owner or the patient has to create an account and then log in to upload the files which can be accessed by the users. The owner provides the time-based access control to the user. The user can access the files to the specified amount of time as allocated by the owner. The user logs into the account, the admin verifies whether the user is authorized person to access the data. If a new user logs in then a new account will be created. Once the user successfully logs into the account, respective files will be searched and displayed. If the files are not present then it will display no files in the server and logs out. To access the data present in the file's user should enter the secrete key. The system checks if it is a correct secret key, if it is, only then the data

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

will be displayed. Otherwise, the user has to log out.

When the user requests for the data, encrypted data will be decrypted and sent to the user. The data can be viewed or edited according to access rights given to the user based on their roles by the owner. This data will be again encrypted and stored in the cloud. In case of emergency, the patient will not be able to activate the user's request. In such scenarios, the secret key required to access the records will be given to the emergency department by the care taker. The time-based access control and role-based accessed control enhances the security feature in the proposed system.

## IV.EXPERIMENTAL RESULTS

An user-friendly interface has been developed to see the practical efficiency of the proposed system. The project is run on Windows 10 of Intel Core i5 processor of 2.40GHz with 8GB memory. We have implemented our scheme in Java/J2EE, the IDE used is Netbeans8.0.1 and the database is used MYSQL. Shamir's Secret Sharing Scheme is employed here to securely split the secrets, which is a built-in function in Java and MD-5 is applied for the hashing function.In our system, the medical report will get uploaded in the cloud. The EHR will be encrypted and stored in the cloud to avoid security threats. The EHR will bedecrypted whenever it has to be downloaded by the user

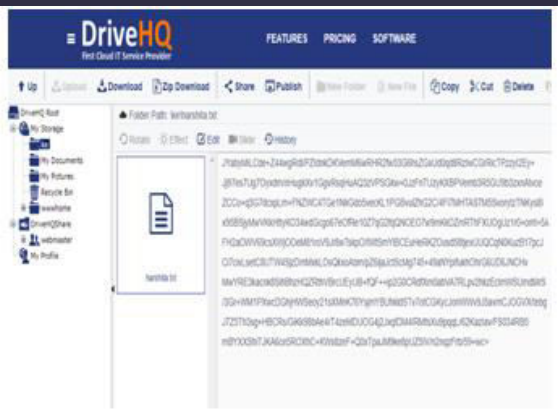


Fig 3: Encrypted medical record


Fig4: Entering the security key page

Fig 2. Shows the decrypted medical records stored in the cloud securely. Fig 3. and Fig 4. depicts the decrypted medical records which can be viewed by the user after entering the respective secret key.


Fig 5: Decrypted medical records

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The proposed system has a time seal feature which limits the access to the EHR for the allocated time. This enhances the security provided to the EHR than the existing system

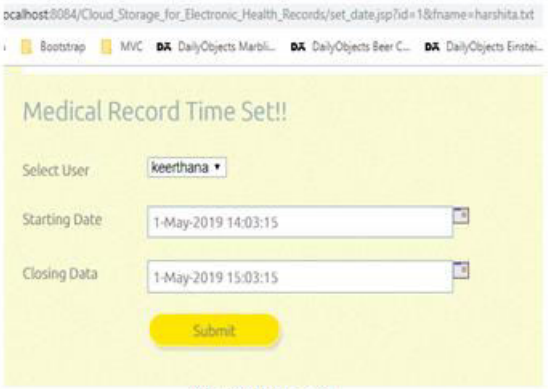

Fig 6: Time seal

Fig 5. Shows the time seal feature in the system. The owner can set the date and time for the particular user for a stipulated amount of time

## V. CONCLUSION

The proposed scheme guarantees the security of the EHR in cloud which is obtained by the use of Shamir's secret key and AES algorithm.The newly added time-based access feature enhances the security by reducing the threats not only from cloud but even from the trusted entities of HCs.

The future analysis requires a moreefficient system which can avoid the inefficient decryption of the records containing images when they are stored in multiple cloud servers. And also user interface can be made more efficient by restricting the manual uploading of EHR.

## REFERENCES

[1] F. Alsolami and T. E. Boult. Cloudstash: Using secret-sharing scheme to secure data, not keys, in multi-clouds. In Proceedings of International Conference on Information Technology: New Generations, pages 315– 320, 2014.

[2] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford. Secure outsourcing of scientific computa-tions. Advances in Computers, 54:215–272, 2002.I.

[3] D. Chaum and T. P. Pedersen. Wallet databases with observers. In Proceedings of Annual International Cryptology Conference, pages 89–105, 1992.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou. New algorithms for secure outsourcing of modular exponen-tiations. IEEE Transactions on Parallel & Distributed Systems, 25(9):2386–2396, 2012.

[5] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong. New algorithms for secure outsourcing of large-scale systems of linear equations. IEEE Transactions on Information Forensics and Security, 10(1):69–78, 2015.

[6] R. D'Souza, D. Jao, I. Mironov, and O. Pandey. Publicly verifiable secret sharing for cloud-based key manage-ment. In Proceedings of Indocrypt 2011, pages 290–309, 2011.

[7] T. Ermakova and B. Fabian. Secret sharing for health data in multi-provider clouds. In Proceedings of Busi-ness Informatics, pages 93–100, 2013.

[8] Hanlin Zhang,Jia Yu,Chenliang Tian,Pu Zhao,Guobin XU and Jie Lin.Cloud storage for Electronic health records based on secret sharing with verifiable reconstruction outsourcing-2016.

[9] T. Ermakova and B. Fabian. Secret sharing for health data in multi-provider

clouds. In Proceedings of Busi-ness Informatics, pages 93–100, 2013.

[10] S. Hohenberger and A. Lysyanskaya. How to securely outsource cryptographic computations. In Proceedings of Theory of Cryptography Conference, pages 264– 282, 2005.

[11] D. Hubbard, M. Sutton, et al. Top threats to cloud computing v1.0. Cloud Security Alliance, pages 1–14, 2010.

[12] J. Lin, W. Yu, and X. Yang. Towards multistep electricity prices in smart grid electricity markets. IEEE Transactions on Parallel and Distributed Systems, 27(1):286–302, 2016.

[13] Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and appli-cations. IEEE Internet of Things Journal, 4(5):1125– 1142, 2017.

[14] A. R. Sadeghi and M. Winandy. Securing the e-health cloud. In Proceedings of ACM International Health Informatics Symposium, pages 220–229, 2010.

[15] S. Salinas, C. Luo, X. Chen, W. Liao, and P. Li. Efficient secure outsourcing of large-scale sparse linear systems of equations. IEEE Transactions on Big Data, PP(99): 1–1, 2017.

[16] C. N. Yang and J. B. Lai. Protecting data privacy and security for cloud computing based on secret sharing. In Proceedings of International Symposium on Biometrics and Security Technologies, pages 259–266, 2013.