ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed(Group –I) Journal Volume 10, Iss 11, November 2021

A NOVEL FRAMEWORK TO PROVIDE SECURITY FOR MEDICAL DOCUMENTS WITH FLEXIBLE ACCESS CONTROL

[1]Cheedella Chandra Sekhar, [2]Kopila Ravi Chand

[1]Assistant Professor, Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali

[2]Assistant Professor, Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali

Abstract: Electronic clinical files (EMRs) play an essential function in healthcare networks. Since these archives continually incorporate substantial touchy statistics related to patients, privateness maintenance for the EMR device is critical. Current schemes generally authorize a person to examine one's EMR if and solely if his/her function satisfies the described get admission to policy. However, these current schemes permit an adversary to hyperlink patients' identities to their doctors. Therefore, classifications of patients' ailments are leaked barring adversaries virtually seeing patients' EMRs. To tackle this problem, we current two nameless schemes. They now not solely gain information confidentiality however additionally recognise anonymity for individuals. The first scheme achieves reasonable security, the place adversaries pick assault goals earlier than acquiring statistics from the EMR system. The 2nd scheme achieves full security, the place adversaries adaptively pick assault ambitions after interplay with the EMR system. We grant rigorous proof displaying the safety and anonymity of our schemes. In addition, we suggest an method in which EMR proprietors can search for their EMRs in an nameless system. For a higher person experience, we practice the online/offline method to pace up records processing. Experimental consequences exhibit that the time complexity for key technology and EMR encapsulation can be decreased to milliseconds

Index Terms—Medical document release, privacy preservation, data authentication, release control.

1.INTRODUCTION

The advanced data gathered by undertakings, open organizations, and governments has made gigantic open doors for information based applications. Driven by these advantages, there exists an appeal for the distribution and trade of gathered information among various parties. Be that as it may, touchy data about clients is normally contained in the first records, and the protection would be abused if such information is discharged without being handled. Archive redaction, a direct strategy for security protecting, is to expel delicate data from the report. For instance, record redaction is a basic methodology for organizations to forestall unintentional or even malevolent divulgence of exclusive development while offering information to redistributed activities. As of late, viable sharing of clinical information has increased noteworthy consideration among experts just as in established researchers. Since this idea holds incredible potential for cultivating the coordinated effort inside the medicinal services network and different gatherings, for

example, pharmaceutical organizations, insurance agencies and research foundations, in order to improve the quality and adequacy of clinical treatment forms. With recent and rapid advancements in communication technologies, digital signals can be transmitted over the internet with convenience [1]. These advancements have brought many advantages but at the same time there are several hazards and risks that need to be considered as well. Technologies such as telemedicine are emerging day by day [2] and ensuring medical data security is becoming a challenge. Recently, capturing medical data has appeared as a major cybercrime. If such sensitive data is stolen or captured, then it can result in violation of basic patient rights. Confidentiality in medical reports must be kept intact in order to ensure trust among patients and health care institutions. Electronic health records (EHR) are stored in large databases of medical institutions, in which patient's health records are kept [3]. These records may include every sort of sensitive information starting from patient's personal data, vital signs, diagnosis reports to laboratory reports etc. This data serves as a medical history for the convenience of doctors and patients. These medical records are shared through modern communication systems which include variety of networks such as local or wide area networks. Out of all the medical information kept in EHRs, 90% data is comprised of medical images. Medical images, such as X-ray, endoscopy images and videos, MR (magnetic resonance) images etc., are stored, handled and transmitted using the Digital Imaging and Communications in Medicine (DICOM) standard. The patient information in DICOM file must be kept confidential to avoid any kind of tampering of patient's data, illegal copying and to guarantee copyright protection [3]. This confidentiality requires medical data to be secured in every way possible.

2.LITERATURE SURVEY

2.1 X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016

With the availability of cloud services, the techniques for securely outsourcing the prohibitively expensive computations are getting widespread attention in the scientific community. That is, the clients with resource-constraint devices can outsource the heavy computation workloads into the untrusted cloud servers and enjoy the unlimited computing resources in a pay-per-use manner. Since the cloud servers may return an invalid result in some cases, one crucial requirement of outsourcing computation is that the client has the ability to verify the validity of computation result efficiently. The primitive of verifiable computation has been well studied by plenty of researchers in the past decades [9], [13], [14], [34], [35], [42], [43], [45]. Most of the prior work focused on generic solutions for an arbitrary function (encoded as a Boolean circuit). Though, in general, the problem of verifiable computation has been theoretically solved, the proposed solutions are still much inefficient for real-world applications. Therefore, it is still meaningful to seek for efficient protocols for verifiable computation of specific functions. Benabbas et al. [19] first proposed the notion of the verifiable database (VDB) in order to solve the problem of verifiable outsourcing storage. That is, assume that a resource constrained client would like to store a very large database on a server so that it could later retrieve a database record and update a

record by assigning a new value. If the server attempts to tamper with the database, it will be detected by the client with an overwhelming probability. Besides, the computation and storage resources invested by the client must not depend on the size of the database (except for an initial setup phase).

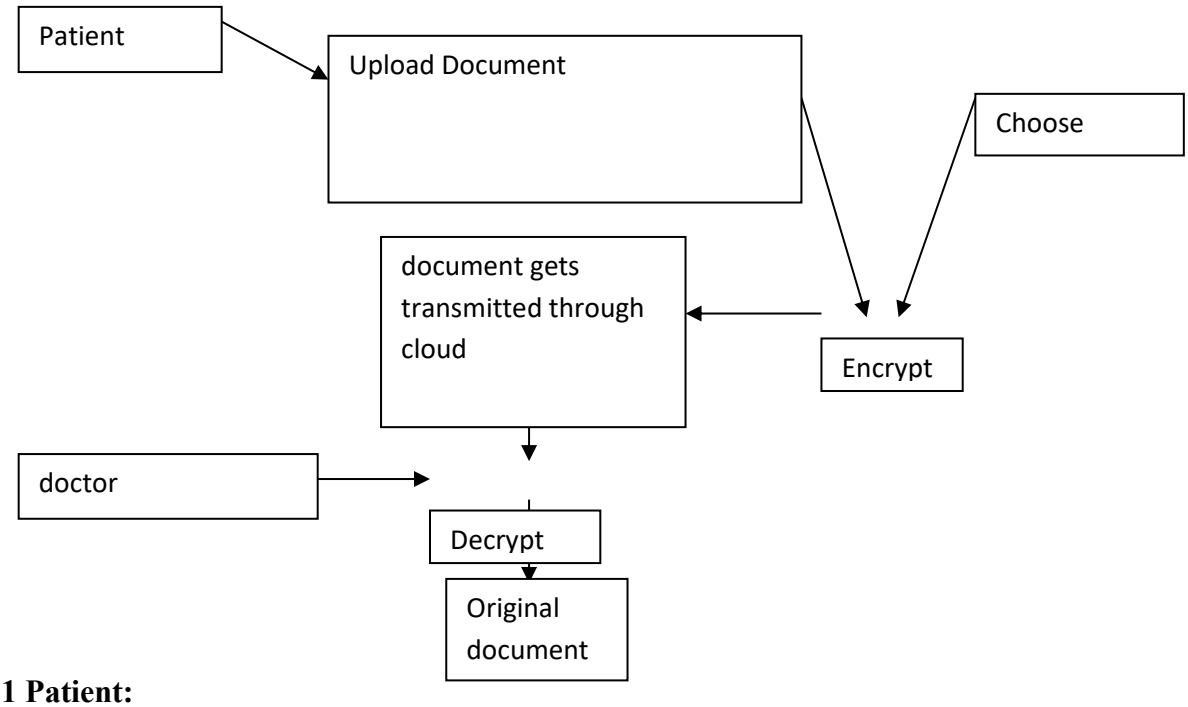
2.2 X. Zhang, T. Jiang, K.-C. Li, A. Castiglione, and X. Chen, "New publicly verifiable computation for batch matrix multiplication," Information Sciences, 2017.

With the prevalence of cloud computing, the resource constrained clients are trended to outsource their computation-intensive tasks to the cloud server. Although outsourcing computation paradigm brings many benefits for both clients and cloud server, it causes some security challenges. In this paper, we focus on the outsourcing computation of matrix multiplication, and propose a new publicly verifiable computation scheme for batch matrix multiplication. Different from traditional matrix computation outsourcing model, the outsourcing task of our scheme is to compute MXiMXi for group of clients, where XiXi is a private matrix chosen by different clients and *M* is a public matrix given by a data center beforehand. Based on the two techniques of privacy-preserving matrix transformation and matrix digest, our scheme can protect the secrecy of the client's private matrix XiXi and dramatically reduce the computation cost in both the key generation and the compute phases. The security analysis shows that the proposed scheme can also achieve the desired security properties under the co-CDH assumption.

2.3 T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, 2016

The development of cloud computing motivates enterprises and organizations to outsource their data to third-party cloud service providers (CSPs), which will improve the storage limitation of resource constrain local devices. Recently, some commercial cloud storage services, such as the simple storage service (S3) [1] on-line data backup services of Amazon and some practical cloud based software Google Drive [2], Dropbox [3], Mozy [4], Bitcasa [5], and Memopal [6], have been built for cloud application. Since the cloud servers may return an invalid result in some cases, such as server hardware/software failure, human maintenance and malicious attack [7], new forms of assurance of data integrity and accessibility are required to protect the security and privacy of cloud user's data. To overcome the above critical security challenge of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme [8] are far from practical application. The formers are not practical because a recent IDC report suggests that data-generation is outpacing storage availability [9]. The later protocols ensure the availability of data when a quorum of repositories, such as k-out-of-n of shared data, is given. However, they do not provide assurances about the availability of each repositories, which will limit the assurance that the protocols can provide to relying parties.

3.PROPOSED WORK



3.1 Patient:

A patient outsources her documents to the cloud server to provide convenient and reliable data access to the corresponding search doctors. To protect the data privacy, the patient encrypts the original documents under an access policy using attribute-based encryption. To improve the search efficiency, she also generates some keyword for each outsourced document. The corresponding index is then generated according to the keywords using the secret key of the secure kNN scheme. After that, the patient sends the encrypted documents, and the corresponding indexes to the cloud server, and submits the secret key to the search doctors.

3.2 Cloud server:

A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

3.3 Doctor:

An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors. When she needs to search the outsourced documents stored in the cloud

server, she will generate a search keyword set. Then according to the keyword set, the doctor uses the secret key to generate a trapdoor and sends it to the cloud server. Finally, she receives the matching document collection from the cloud server and decrypts them with the ABE key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way. For simplicity, we just consider one-way communication in our schemes.

4.RESULTS AND DISCUSSION

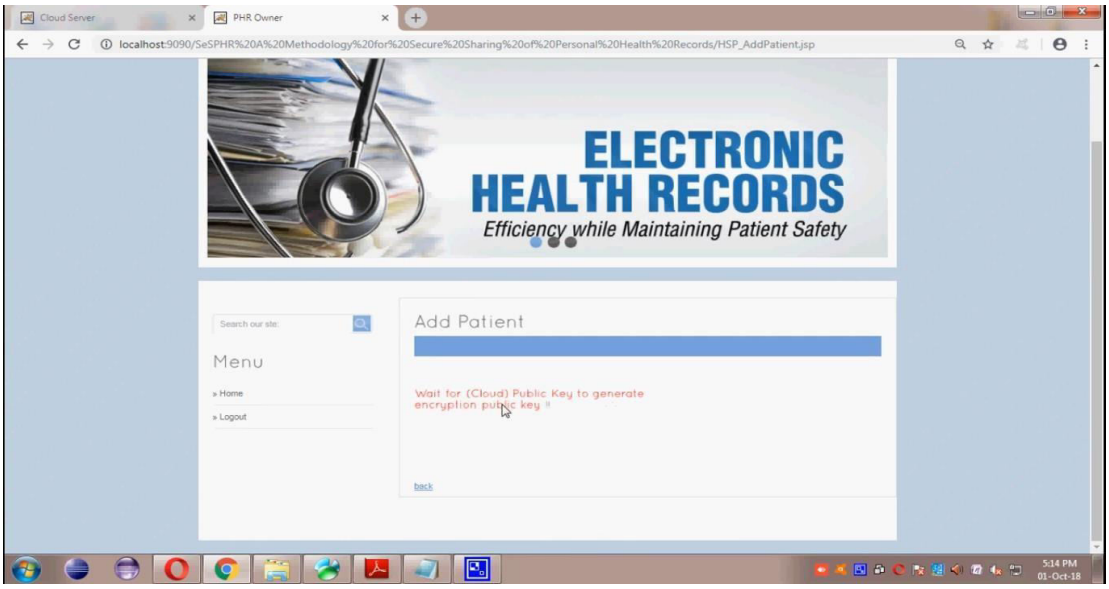


Fig 1: Patient sending encryption req to cloud

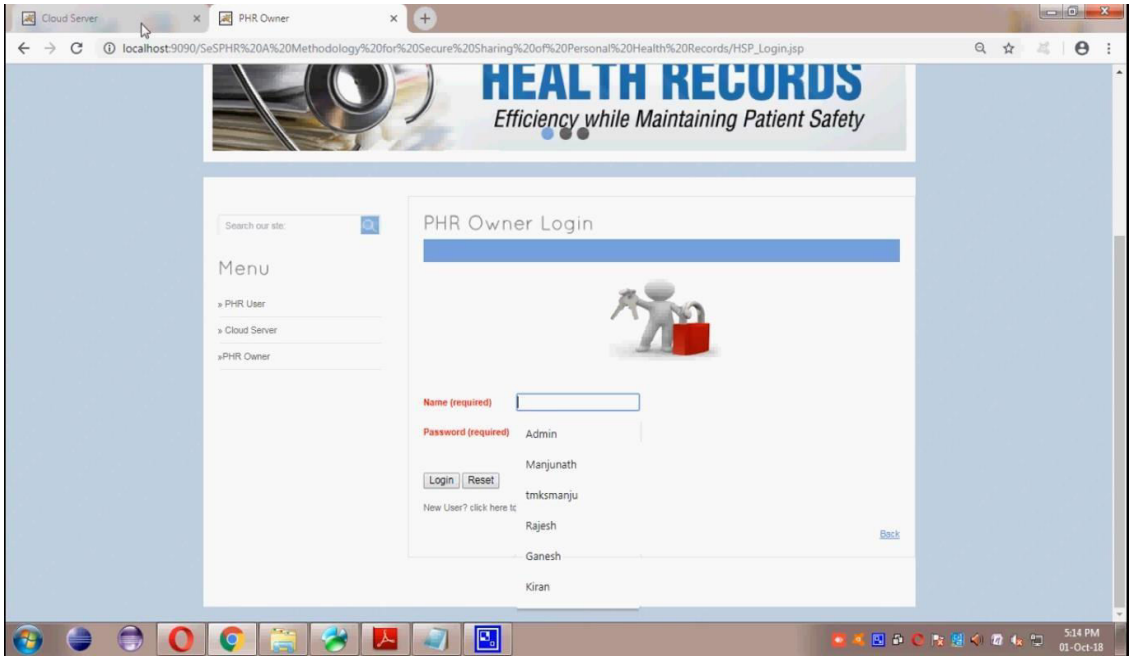


Fig 2:PHR owner Form

5.CONCLUSION

We proposed a methodology to securely save and transmission of the PHRs to the approved entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric get right of entry to manage to one-of-a-kind parts of the PHRs based totally on the get admission to furnished by way of the patients. We applied a fine-grained get admission to manage technique in such a way that even the valid machine customers can't get right of entry to these parts of the PHR for which they are no longer authorized. The PHR proprietors shop the encrypted statistics on the cloud and solely the approved customers possessing legitimate re- encryption keys issued by using a semitrusted proxy are in a position to decrypt the PHRs.

The position of the semi-trusted proxy is to generate and shop the public/private key pairs for the users in the system. In addition to keeping the confidentiality and making sure patient-centric get entry to manipulate over the PHRs, the methodology additionally administers the ahead and backward get admission to manage for departing and the newly becoming a member of users, respectively. Moreover, we formally analyzed and demonstrated the working of SeSPHR methodology thru the HLPN, SMT-Lib, and the Z3 solver. The overall performance assessment was once executed on the on the foundation of time fed on to generate keys, encryption and decryption operations, and turnaround time. The experimental outcomes show off the viability of the SeSPHR methodology to securely share the PHRs in the cloud environment.

REFERENCES

[1] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[3] 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, vol. 10, no. 1, pp. 69–78, 2015.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secure outsourcing of modular exponentiations,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2386–2396, 2014.

[5] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, “Verifiable auditing for outsourced database in cloud computing,” IEEE transactions on computers, no. 1, pp. 1–1, 2015.

[6] T. Jiang, X. Chen, and J. Ma, “Public integrity auditing for shared dynamic cloud data with group user revocation,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, 2016.

[7] X. Zhang, T. Jiang, K.-C. Li, A. Castiglione, and X. Chen, “New publicly verifiable computation for batch matrix multiplication,” Information Sciences, 2017.

[8] R. Johnson, D. Molnar, D. Song, and D. Wagner, “Homomorphic signature schemes,” in Cryptographers’ Track at the RSA Conference. Springer, 2002, pp. 244–262.

[9] G. Becker, "Merkle signature schemes, merkle trees and their cryptanalysis," Online im Internet: http://imperia.rz.rub.de, vol. 9085, 2008.
[10] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," Journal of the ACM (JACM), vol. 33, no. 4, pp. 792–807, 1986.
[11] R. Steinfeld, L. Bull, and Y. Zheng, "Content extraction signatures," in International Conference on Information Security and Cryptology. Springer, 2001, pp. 285–304.
[12] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, and S. Tezuka, "Digitally signed document sanitizing scheme with disclosure condition control," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 88, no. 1, pp. 239–246, 2005.
[13] K. Miyazaki, G. Hanaoka, and H. Imai, "Digitally signed document sanitizing scheme based on bilinear maps," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ACM, 2006, pp. 343–354.
[14] J. L. Brown, "Verifiable and redactable medical documents," Ph.D. dissertation, Georgia Institute of Technology, 2012.
[15] H. C. Pöhls, A. Bilzhause, K. Samelin, and J. Posegga, "Sanitizable signed privacy preferences for social networks," DICCDI, LNI. GI, 2011.
[16] H. C. Pöhls and M. Karwe, "Redactable signatures to control the maximum noise for differential privacy in the smart grid," in International Workshop on Smart Grid Security. Springer, 2014, pp. 79–93.

Author Profiles:

Ms. VADA PRATHYUSHA pursuing M.Tech in computer science and engineering from NARAYANA ENGINEERING COLLEGE, Nellore affiliated to the Jawaharlal Nehru Technological University, Anantapur in 2018-20, respectively.

Mr S. Tamilselvan, B.E, M.E, (Ph.D)., Associate Professor, Narayana Engineering College, Nellore, in the area of Image Security. His area of interest is image Security, Cloud Security