*International Journal for Modern Trends in Science and Technology*, 9(SI01): 91-94, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST09SI0117
Available online at: http://www.ijmtst.com/vol9si01.html

# A Remarkable Structure to Ensure the Safety of Medical Documents while Allowing for Adaptable Access Control

**T.Shalini, CH.Deepika, T.Karuna Latha, P.Madhavi**

Department of Computer Science and Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada.

**To Cite this Article**
T.Shalini, CH.Deepika, T.Karuna Latha, P.Madhavi. A Remarkable Structure to Ensure the Safety of Medical Documents while Allowing for Adaptable Access Control. International Journal for Modern Trends in Science and Technology 2023, 9(SI01), pp. 91-94. https://doi.org/10.46501/IJMTST09SI0117

**Article Info**
Received: 26 January 2023; Accepted: 22 February 2023; Published: 26 February 2023

## ABSTRACT

***EMRs (electronic medical records) serve a critical purpose in healthcare systems. The EMR device must maintain patient privacy because these archives contain sensitive information about patients on a regular basis. Current policies normally allow an individual to look at another's EMR if and only if his or her role matches the criteria mentioned in the policy's entry to. The present systems, on the other hand, allow an adversary to link the identities of patients to their doctors. To prevent opponents from viewing the electronic medical records (EMRs) of patients, the classifications of their ailments are leaked. We have two unnamed schemes in place to address this issue. As a result, they've gained not only information secrecy, but also individual anonymity. The first strategy provides a decent level of security by allowing attackers to select their attack objectives prior to accessing EMR system data. After interacting with the EMR system, enemies are able to alter their attack plans based on their interactions with the EMR system. In order to demonstrate our systems' security and anonymity, we provide extensive documentation. EMR owners can use our method to find their own records in a nameless database. We use the online/offline approach to speed up record processing in order to provide a better user experience. EMR encapsulation and key technology have demonstrated experimentally that their time complexity may be reduced to milliseconds.***

## 1.INTRODUCTION

The advanced data collected by businesses, open groups, and governments has made enormous open doors for information-based applications to be used in their systems. As a result of these benefits, the sharing and exchange of obtained information among multiple parties has gained popularity. The sensitive information about clients is usually kept in the earliest records, thus releasing it without first handling it would be a misuse of the protection. In order to secure sensitive information, archive redaction is a straightforward method of doing so. When it comes to protecting proprietary information from unintended or malicious leaks, record redaction is a go-to solution for many firms. Clinical information

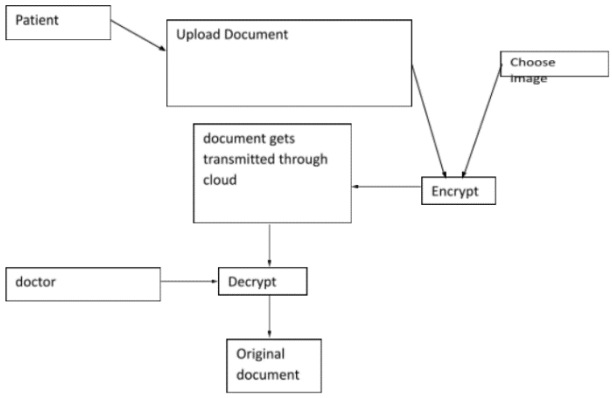
exchange has recently gained significant attention from professionals and established researchers alike. In order to boost clinical treatment quality and adequacy, this concept has enormous potential for cultivating a coordinated effort within the medical services network as well as various gatherings, such as pharmaceutical organizations, insurance agencies, and research foundations, for example. Transmitting digital signals via the internet has never been easier, thanks to recent and rapid improvements in communication technologies. Many benefits have resulted from these developments, but there are also a number of dangers and concerns to be aware of. Every day new technologies like telemedicine emerge, making medical data security a concern. Medical data theft has recently become a major cybercrime. Patients' basic rights may be violated if such private information is taken or intercepted. In order to maintain patient and medical institution confidence, the confidentiality of medical records must be protected. Medical institutions use electronic health records (EHR) to maintain patient health records in massive databases [3]. Patients' personal data, vital signs, diagnosis reports, and laboratory tests are just a few examples of sensitive information that may be included in these records. Patients and clinicians can use this information to create a medical history. It is possible to share medical records using a variety of current communication methods, including local and wide area networks. Medical photographs make almost 90% of the data stored in electronic health records (EHRs). Digitized imaging and communications in medicine (DICOM) standards are used to store and transmit medical images, including X-ray and endoscopic images as well as MR (magnetic resonance) images. The patient information in DICOM file must be maintained confidential to avoid any kind of tampering of patient's data, unauthorized duplication and to guarantee copyright protection [3]. Medical records must be protected in every manner possible in order to maintain this level of privacy..

## 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

[17] The scientific community is paying increased attention to methods for safely outsourcing formerly prohibitively expensive computations now that cloud services are widely available. A pay-per-use model allows customers with resource-constrained devices to outsource their computationally intensive workloads to untrusted cloud servers. One of the most important aspects of outsourcing computation is that the client has the ability to quickly and easily verify the validity of the computation output. [9], [13], [14], [35], [42], [43], [45] have all done extensive study on the verifiable computation primitive. It was once common to develop generic solutions for any function (encoded as a Boolean circuit). But even if in theory verifiable computation has been solved, the proposed techniques are far too slow for real-world use. Hence, the pursuit of efficient protocols for the verifiable computation of certain functions is still relevant.... It was first proposed by Benabbas et al. [19] that a verifiable database (VDB) solve the problem of verifiable outsourcing storage. So, let's say a resource-constrained client wants to store a huge database on the server for subsequent retrieval and updating of database records through the assignment of new values. This is an example of database scalability. The client will almost certainly notice any attempts by the server to tamper with the database. Furthermore, the client's investment in computing and storage resources should not be dependent on the database's size (except for an initial setup phase).

## 3. PROPOSED WORK




3.1 Patient:

A patient uses a cloud server to save and share her documents with the appropriate search doctors, making it easy for them to access and use. The patient uses attribute-based encryption to encrypt the original

documents in order to maintain the confidentiality of the information. Additionally, she generates a keyword for each outsourced paper. The secret key of the secure kNN technique is then used to construct the corresponding index based on the keywords. Patient then delivers encrypted papers to the cloud server and provides a secret key to search doctors. Documents and indexes are then sent to the cloud server.

3.2 Cloud server:

Cloud servers are intermediary entities that store encrypted documents and indexes received from patients, and then provide search services for authorized search doctors to access and search the data. It is possible for the cloud server to return a group of matching papers to a search doctor when he or she submits the information to it..

3.3 Doctor:

The mystery key may be acquired from the affected person with the aid of using a certified physician, and trapdoors may be generated the usage of this key. A seek key-word set may be generated whilst she wishes to look outsourced files saved at the cloud server. A trapdoor is then generated and dispatched to the cloud server with the aid of using the physician the usage of the name of the game key consistent with the key-word selected. In the end, she obtains the matched file series from the cloud server and makes use of the ABE key acquired from the straightforward authority to decrypt the files. [18] The physician also can outsource clinical reviews to the cloud server after receiving the affected person's fitness information. To preserve matters simple, all of our structures count on one-manner communication.

**4. RESULTS**

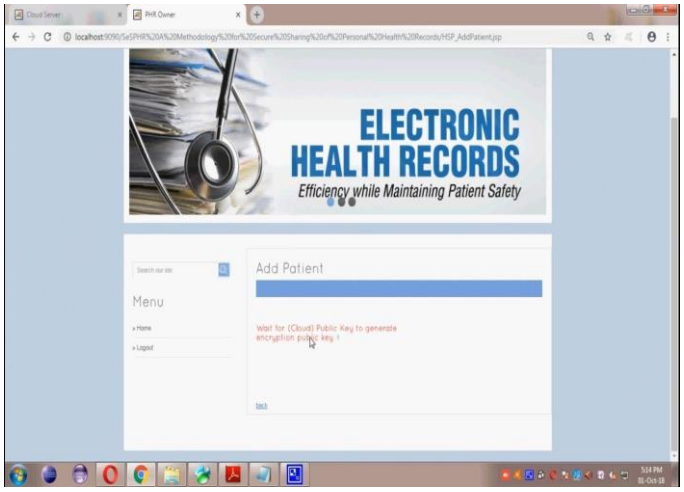



Fig 1: Patient sending encryption req to cloud

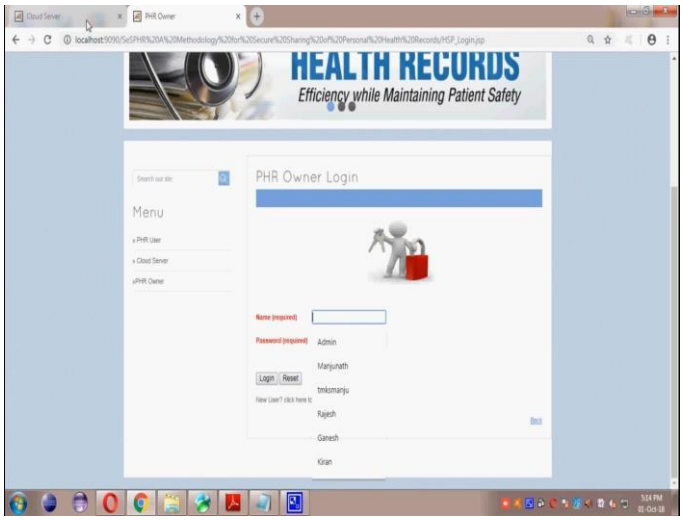



Fig 2:PHR owner Form

**5. CONCLUSION**

We devised a strategy for storing and transmitting PHRs to authorized cloud service providers in a safe manner. The method protects the privacy of personal health records while allowing patients to control access to specific elements of their records based only on the permissions they provide. Because we used a fine-grained access control method, no one, not even authorized machine users, may access those parts of the PHR that were previously accessible to them. The PHR owners store encrypted data in the cloud, and only those customers who have been granted access to the PHRs by a semi-trusted proxy can decode them.

Key generation and storage are handled by the semi-trusted proxy on behalf of system users. Aside from maintaining confidentiality and ensuring patient-centric access to PHRs, the technique also administers the forward and backward access to manage for outgoing

and newly enrolled users. SeSPHR approach was explicitly tested and shown using the HLPN, SMT-Lib, and Z3 solvers. It was originally done using the time it took to produce keys, perform encryption and decryption operations, and the turnaround time for the entire process. The results of the experiments suggest that the SeSPHR approach may be used to securely distribute PHRs in the cloud.

### Conflict of interest statement

Authors declare that they do not have any conflict of interest.

## 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] [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

[17] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[18] Kumar, J. R., Sujatha, B., &Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing."