iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.40089

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com

Secure Integrity Auditing System for Electronic Patient Health Records using Advanced Encryption Techniques

Kulkarni Vaibhav G.[1], Bidve Manisha P.[2]
[1]*DBAT University,* [2]*Asst. Professor, Department of CE, M.S.Bidve Engineerin College, Latur, Maharashtra, India*

Abstract: ***Cloud computing is one of evolving technology nowadays, giving versatile services. However, secure information sharing is vulnerable to cloud computing. With cloud storage services, users can remotely keep their information to the cloud and recognize the data sharing with others. Electronic wellbeing record (EHR) is a framework that gathers patients' computerized wellbeing data and offers it with other medical care suppliers in the cloud. Since EHR contains a lot of critical and delicate data about patients, it is necessitated that the framework guarantees reaction accuracy and capacity respectability. The verifiable database (VDB), where a user's redistributes his huge data set to a cloud worker and makes questions once he needs certain information, is proposed as an effective updatable distributed storage model for asset compelled users. To improve productivity, most existing VDB plans use confirmation reuse and evidence refreshing strategy to demonstrate accuracy of the question results. Notwithstanding, it overlooks the "continuous" of confirmation age, which brings about an overhead that the user needs to perform additional cycle (for example evaluating plans) to check stockpiling trustworthiness. In this paper, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving using secure encryption and batch integrity checking.***

Keywords: cloud storage, data integrity auditing, functional commitment, privacy-preserving auditing, sensitive information hiding, third-Party Auditor (TPA), user revocation Verifiable database.

I. INTRODUCTION

The cloud services industry has expanded unprecedentedly with the exponential increase in global knowledge. Many cloud providers are in the process of launching cloud services and products, including Am-azon, GOOGLE, Alibaba, Huawei and Microsoft. People start to supply the cloud service providers with their massive data storage tasks (CSPs). It no longer limits them to a small amount of local storage and computer resources. As a concrete and high-quality example of cloud storage, many organisations, like the United-States National Coordinator for Health Information Technology are strongly supporting the cloud-based electronic health records (CB-EHR), a system which collects the patients' digital health information. The patient EHRs can be accessed and updated later on the workstation or mobile device. Different medical institutions can exchange patient EHRs uploaded into the cloud to assist patients in better care, assist scientists in the study of diseases and re-searches, and support departments of public health forecast, track and potentially deter the outbreak of infectious diseases. As an independent management agency is the cloud service provider (CSP), consumers literally relinquish the absolute control of their EHRs. This poses security problems in the externalization of activities. For example, for a variety of reasons cloud servers will return false results, such as cloud malfunctioning and the attack by a hacker. The incorrect value returned may have a significant effect on all aspects of the medical system. The main issue with the EHR method is therefore how to check each time the server answers correctly.

Electronic Health Record Systems (CB-EHR) based on the cloud are increasing now a days. There are three traditional CB-EHR systems: data owners, suppliers of data and a Cloud server. Data owners and data providers are specified in the CB-EHR framework as both patients and hospitals. Data owners may allow data providers to download their EHRs directly to the cloud. The CB-EHR framework provides data owners with a more complete overview of their EHRs every time and everywhere, better equipped for medical meetings and unforeseen emergencies, a better image on personal health and fitness targets. Through the sharing, collaboration and engaging of patients in different ways data providers can explore the CB-PHR framework to provide improved medical services.

We propose in this paper a highly efficient CB-EHR scheme that guarantees good privacy. Each data owner in our system allowed multiple data providers to supply the cloud server with encrypted health records and data indices. In two desirable features, our system differs from previous work. First of all, a special, symmetrical key is used by each data provider from the same data owner for data index encryption, thus resisting a single point. Secondly, every data owner does not need to manage the keys with individual health providers and can send a single encrypted query to the cloud server to check all his data suppliers for encrypted health data. The second function makes query processing very effective.

II. RELATED WORK

Boyang Wang et al [1] "Privacy preserving public Auditing for shared data in the cloud" In this paper, the identity of the signatories on each block of shared knowledge is intact personal from public verification, verifying the functionality of shared knowledge integrity without retrieving the entire file. In addition, it is ready to perform multiple auditing tasks simultaneously instead of confirming one after the other. The scheme uses a ring signature to create a homomorphism authentication so that the public verifier is able to audit the shared data integrity without retrieving the entire data, yet cannot identify who is the signatory on each block. But the scheme is unable to handle 1. Traceability - means the ability of the group manager to reveal the identity of the signer based on verification metadata in certain special circumstances. 2. How to prove the freshness of data.

Tina Esther Trueman et al [2] Ensuring privacy and data freshness for public auditing of Shared data in cloud" In this paper, it uses a new method to create specific privacy and data freshness of shared knowledge in cloud exploitation. The Holomorphic Authenticable Ring Signature (HARS) theme is used to protect user privacy and the Cover Tree Rules are used to ensure users have the required level of freshness information. Also, a third party auditor (TPA) audits the information stored in the cloud. It should be able to verify the credibility of the CSP without revealing the identity of the users in the group. The disadvantage is that malicious activities by the user cannot be detected. The difficulty of this system is to increase the traceability, which means that only the genuine user can verify the identity of the signer so that the malicious entertainment done by the user in the group can be maintained.

Rongxing Lu et al [3] "Toward Efficient and Privacy- Preserving Computing in Big Data Era". In this paper, it is introducing an efficient and privacy-protecting cosine equivalence (PCSC) computer protocol in response to data mining efficiency and privacy requirements in the Big Data era. The proposed PCSC protocol is not only confidential but also efficient. This is especially true for big data analysis. The advantage is that the calculation of the proposed PCSC protocol will increase even when the overhead n is large.The downside is that certain privacy needs to be provided for certain big data analytics. Privacy is introducing computing-like protocols to provide complete and unique protection in the big data age.

S. Fugkeaw et al [4] Privacy-preserving access control model for big data Cloud". In this paper, it integrate access manages that combine role-primarily access control (RBAC) versions, symmetric encryption, and cipher text attribute-based holistic encryption (CP-ABE) to support micro-access control for large data outsourced to cloud storage systems. They also demonstrate the efficiency and overall performance of our proposed plan through implementation.

J. Yu et al [5]: Enabling Cloud Storage Auditing with Verifiable Out-sourcing of Key Updates." In this paper, the major updates are often accurately outsourced to certain official parties and as a result the burden of important things-updates on the protectors will be kept to a minimum. Third-party auditors (TPAs) in many of the present public auditing designs, in our case, allow legitimate celebration functions and make each storage at the rate of auditing and therefore relaxed key updates for key-exposure resistance. In this technique, the TPA must maintain the encrypted model of the client's secret key while fulfilling these burdensome responsibilities on behalf of the client. The simplest client needs to download the encrypted mystery key from TPA when uploading new files to the cloud. In addition, this layout equips customers with the functionality to verify the validity of encrypted mystery keys provided using TPA. One problem with this system is that TPA needs to outsource calculations for major updates because TPA does not understand the important secret key of the protector.

Tejaswani et al. [6] has proposed a "Privacy preserving public verifiability for integrity of data storage in cloud computing". In this paper, Data privacy is achieved using the Merkel hash tree and RSA-based cryptography algorithms. In this proposed method, the user first generates a public and private key and then encrypts the file with a computer signature on the encrypted file. User sent signature and public key to TPA. TPA then creates a task and sends it to the server. The server calculates the return and provides the TPA. The TPA then checks the integrity of the data by comparing the response with the signature. The proposed approach is safe. Also, data integrity and confidentiality are achieved. It does not support data dynamics with batch auditing.

J. Yuan and S. Yu, [7] "Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification". In this paper, a single cloud node is used by tracked users to track the last updated authentication tag. In this case, if the cloud node responsible for the tag update is negotiating due to some internal bugs or external attacks, the canceled user will be able to get the legal authentication tag.

Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, [8] "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing". In this paper, It has proposed a design that allows users to monitor data stored in cloud storage. This technique can only be useful for finding modified blocks using the homomorphic token pre-computation technique and then using the eraser coded method to retrieve selected blocks from multiple servers. It uses pre-compiled verification tokens to complete data storage accuracy and data error localization simultaneously.

K. He, C. Huang, J. Shi and J. Wang, [9] "Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage". In this paper, it proposes a scheme in which the data owner first encrypts the information file using the renewal code and then the coded file will be transversely stored on multiple cloud servers. Multiple cloud servers can suggest the same service provider or different service providers. The data owner can perform block-level dynamic operations to modify, add, and delete blocks on outsourced data. Auditors can cleverly standardize the integrity of data stored on multiple cloud servers; Again, data files are frequently updated by the data owner. The confidentiality and integrity of the data stored in the cloud is a hallmark of reputation in cloud computing.
S. More and S. Chaudhari, [10] "Third Party Public Auditing Scheme for Cloud Storage". In this paper, a mechanism using MHT and RSA algorithms is proposed. In their system, it has implemented a system that provides public auditability only for static data. If the owner makes some changes to the original file, TPA will not be able to give proper results. Again, failed to provide batch auditing.

III. OPEN ISSUES

A lot of work has been done in this field thanks to its extensive use and applications. This section mentions some of the approaches that have been implemented to achieve the same purpose. These works are mainly differentiated from the techniques for auditing systems. Unauthorized entities may gain malicious access to EHRs without consent of patients, which has detrimental impacts on data integrity, privacy and security of cloud e-health systems. Moreover, patients may find it difficult to track and manage their health records shared among healthcare providers on clouds. The cloud sever will honestly perform the data requests, but meanwhile will obtain personal information without consent of users, which leads to serious information leakage issues and network security.Now days, preserving sensitive health information against potential threats become big problem.

IV. CONCLUSION

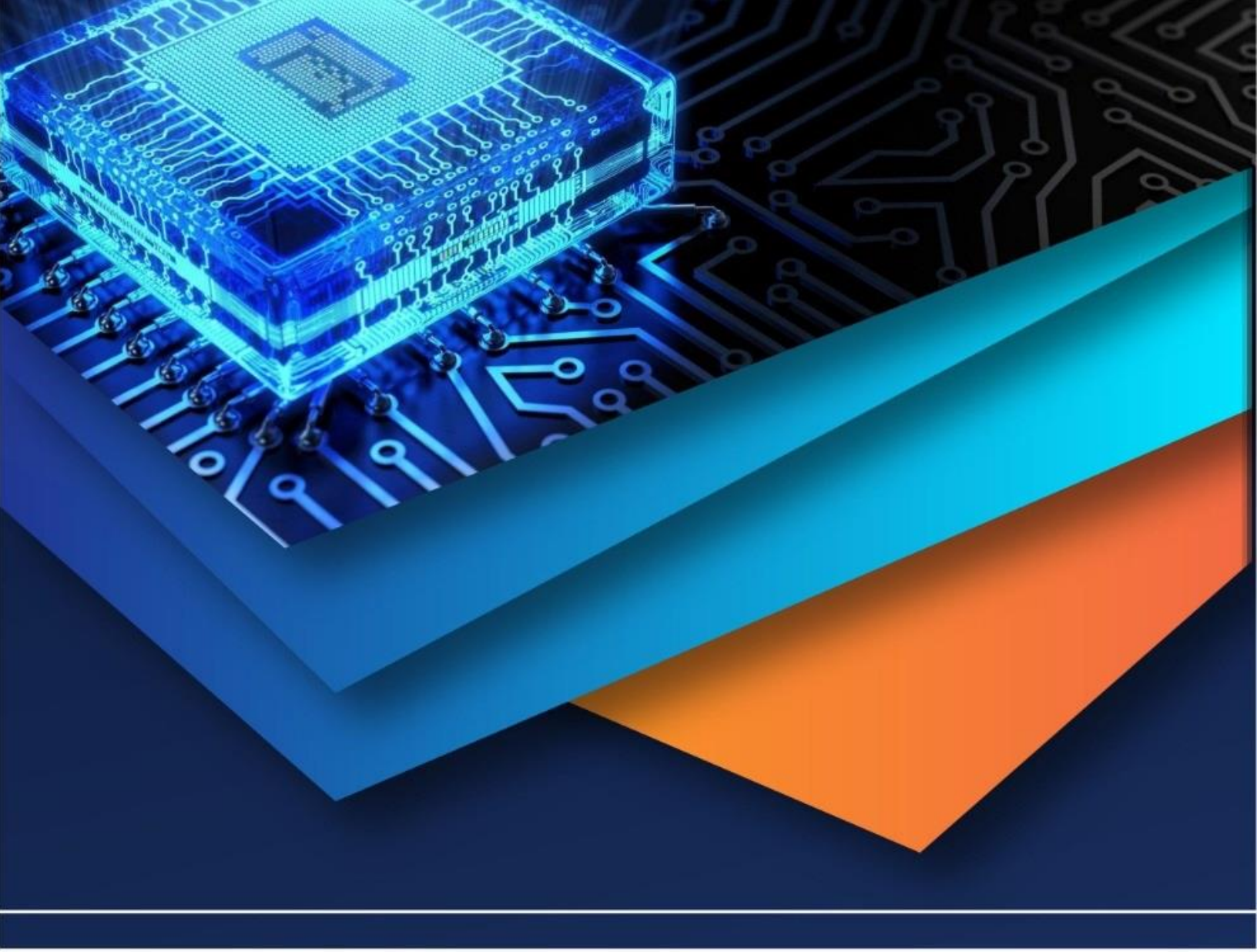
A very useful method for verifiable EHR storage is the verifiable database principle. Yet reuse of facts and server updating technologies to maximize device performance and Data accuracy inspection struggles to achieve. In this piece, we are suggesting a new VDB update scheme based on the Functional commitment to protecting privacy Auditing for honesty and member activities Join and exclude. Two EHR safety standards Implemented: right server answer and Integrity in data stocking. Our VDB system is the right thing to do without too much machine rise, protection priorities. And this is our VDB scheme Minimum cost for terminal connectivity with Output is limited.

V. ACKNOWLEDGMENT

Express my true sense of gratitude, to my guide of the project Prof. M. P. Bidve for her precious collaboration and guidance that she gave me during my research, to inspire me and provide me with all the laboratory facilities. She allowed me to carry out this research work in a very simple and practical way. I would also like to express my thanks to our HOD. Prof. S.R. Tandle, Coordinator Prof. N. J. Pathan, and Principal Prof. B. V. Dharne and all my friends who, knowingly or unknowingly, helped me during my hard work.

REFERENCES

[1] Boyang Wang, Baochun Li,Hui Li, "Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.
[2] Tina Esther Trueman ,P.Narayan asamy "Ensuring privacy and data freshness for public auditing of Shared data in cloud," 2012:
[3] Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, Jun Shao , "Toward Efficient and Privacy-Preserving Computing in Big Data Era " July/August 2014
[4] S. Fugkeaw , H. Sato, Chiang Mai , "Privacy-preserving access control model for big data Cloud", International Computer Science and Engineering Conference (ICSEC), 2015, pp. 1-6.
[5] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.
[6] Tejaswini, K. Sunitha, and S. K. Prashanth, ―Privacy preserving and public auditing service for data storage in cloud computing,‖ ParipexIndian Journal of Research, vol. 2, no. 2, pp. 131–133, Jan. 2012.
[7] J. Yuan and S. Yu, ―Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification,‖ IEEE Transactions on Information Forensics and Security 2015.
[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ―Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,‖ IEEE Transactions on Parallel and Distributed Systems, 22(5):847–859, 2011.
[9] K. He, C. Huang, J. Shi and J. Wang, ―Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage,‖ IEEE Symposium on Computers and Communication (ISCC), 2016.
[10] S. More and S. Chaudhari, ―Third Party Public Auditing Scheme for Cloud Storage,‖ Procedia Computer Science, vol. 79, pp. 69–76, 201



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY