|| Volume 6 || Issue 6 || June 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

EFFICIENT PRIVACY-PRESERVING INTEGRITY AUDITING SYSTEM FOR ELECTRONIC HEALTH RECORDS USING SECURE ENCRYPTION ALGORITHMS

Mr. Ajitkumar Kadam[1], Prof. Vandana Navale[2]

PG Student, Computer Engineering, Dhole Patil College of Engineering, Pune, India[1]

Faculty, Computer Engineering, Dhole Patil College of Engineering, Pune, India[2]

ajitkumar.kadam@gmail.com[1], vandananavale@dpcoepune.edu.in[2]

Abstract: Cloud computing is now one of the most advanced and versatile solutions in technology. But secure sharing of information is cloud computing vulnerable. Users can keep information in the cloud remotely and recognize the sharing of data with others using cloud storage services. 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 Amazon, 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 organizations, 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 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] Public protection of privacy Check for shared cloud data" In this article, the identity of the signing party is unbroken personal from public verifications on every block of shared knowledge, and effectiveness verifies the integrity of shared knowledge while not finding the whole file. Moreover, it is ready to carry out multiple audit tasks simultaneously instead of one by one confirming them. The ring signatures in this system are used to build homomorphic authenticators so that a public auditor can audit the integrity of the shared data without recovering all data. But it cannot handle this scheme 1. Traceability-that is the group manager's capacity to show the signator's identity in specific situations based on verification metadata. 2. Data accuracy proof.

Tina Esther Trueman et al [2] Protection of data and privacy for the public audit of shared data in the cloud" It uses a new method to make shared knowledge of data protection and data refreshments in the cloud theme for the conservation of user privacy and Holomorphic authenticated signature (HARS) The tree overlay rule is used to ensure that the information is fresh to users. The Third Party Auditor (TPA) also audits the cloud's information. You need to be able to monitor the CSP's confidence without revealing the identity of the group's users. The downside is that malicious user activities cannot be detected. The problem with the system is to increase traceability, meaning that only the authentic user can monitor the signator's identity to preserve the malicious pastime that is made through the user in the group.

Rongxing Lu et al [3] Big Data Era computer preservation Efficient and Privacy In response to efficiency and data mining privacy needs in the Big Data era, an effective and privacy-preserving cosine similarity (PCSC) computer protocol was introduced. The PCSC protocol proposed does not only maintain privacy, but is also effective. In Big Data Analytics it is especially suitable. The gain is also increased when n is large by the compute overhead for the proposed PCSC protocol. The downside is that certain big data analytics need to have special privacy. Protocol introduction such as data protection computers to ensure complete and unique protection in the age of big data.

S. Fugkeaw et al [4] Model Big Data Cloud privacy-preserving access control:" Propose a unique access management model combining role-basic Access Control (RBAC) version, symmetric encryption and fully encrypted (CP-ABE) text-based attribute chips to support a thorough access control for large, cloud storage facts outsourced. We also demonstrate through implementation the efficiency and overall performance of our proposed system.

J. Yu et al [5]: Enables the audit of cloud storage by verifiable key update outsourcing.: Here, the important update burden on the employer will be kept minimal, often with accurate outsourcing to a handful of licenced parties. In many current public auditing plans, the third-party auditor (TPA) allows us to play the function of legal celebration and to make the storage audit rates and thus the relaxed key updates for key exposure resistance. In this technique, TPA simple should retain, in the same time as fulfilling these burdensome obligations on behalf of the customer, an encrypted model of customer secret key. When you download new files into the cloud the simplest consumers must download an encrypted mystery key from the TPA. Except that this layout further enables the consumer to check the validity by the TPA of the encrypted mystery keys. One hassle of this system is that the TPA must carry out out the outsourcing of key updating calculations because the TPA does not understand the patron's important secret key.

Tejaswani et al. [6] has Proposed confidentialité preserving public verifiability of cloud data storage integrity using Merkle's hash tree whereas RSA-based cryptography algorithms ensure data confidentiality. User generates a public and private key in this proposed method and then encrypts a file together with computer signature over an encrypted file. The signature and public key were forwarded by the user to TPA. TPA creates and sends a task to the server afterwards. The server calculates and provides TPA with the comeback. Later TPA verifies the integrity of the data compared to the signature response. The approach proposed is safe. Data are also guaranteed integrity and confidentiality. It does not support data dynamics along with batch auditing.

Yuan et al. [7], The validation tag that was last updated for the users rescinded is maintained using a single cloud node. In this situation, the revoked user can produce legal validation tags if the cloud node that is responsible for Tag update is negotiated due to a number of inside failures or outdoor attacks.

Wang et al. [8] has also proposed to allow users to review the data stored in cloud storage. This technique can help you to detect modified blocks by simply using the pre-calculation technique of a holomorphic token, and then delete the coded method to get the selected block from several servers. It uses pre-compiled verification tokens to achieve data storage correctness and location errors simultaneously.

He et al. [9] the scheme proposed in which the data owner initially encrypts the data file by using renewal code, then encoded file is transversely stored on several cloud servers. Similar service providers or different providers may propose multiple cloud Servers. As a bloc alteration, insertion and deletion, the data owner can perform a dynamical block-level

operation on outsourced data. Cleverly, the auditor could authenticate data integrity that is stored on several cloud servers; again, the data file is often updated by the owner of the data. In cloud computing the secrecy and honesty of cloud-specified data is the reputation.

More et al. [10] has proposed using an algorithm MHT and RSA. It has introduced a system in its system that provides only static data for public auditability. The TPA cannot give an appropriate result if the owner changes the original file. Again, batch auditing cannot be performed.

III OPEN ISSUES

Thanks to its extensive use and applications, many works has been done in this field. This section discusses some of the approaches to achieve the same goal. These works differ primarily from the privacy techniques that protect the integrity of audit systems.

Sr no	Parameter	Existing system	Proposed System
1	Security	Use traditional algorithm for encryption.	Propose advanced encryption algorithms for data security.
2	data sharing with sensitive information hiding	No	Yes
3	Data Integrity	No	Yes
4	Block Level	No	Yes

IV CONCLUSION

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.

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, 2016.