JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE INTEGRITY AUDITING SYSTEM FOR PATIENTS HEALTH RECORDS USING ADVANCED ENCRYPTION TECHNIQUES

Mr. Vaibhav G. Kulkarni
Student, Department of Computer Engineering
M. S. Bidve Engineering College, Latur.
vgkulkarni9309@gmail.com

Prof. Manisha P. Bidve
Professor, Department of Computer Engineering
M. S. Bidve Engineering College, Latur.
manishabidve2@gmail.com

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 users 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.

Index Terms—**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 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 externalisation 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 everytime 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.

A. Motivation

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.

B. Objectives

To improve data privacy and data security using Encryption Algorithms.
To provide efficient management of e-health records on clouds.
To improve the security using advanced encryption tech-niques
To achieve Access Control within the group private keys are generated for every user to provide access to files.
To achieve data confidentiality after revocation of any member the private keys of existing members of that group will be update privacy references.

II. HISTORY & BACKGROUND

Boyang Wang et al [1] Privacy preserving public Auditing for shared data in the cloud” In This paper, the identity of the signer on every block in shared knowledge is unbroken personal from public verifies, efficiency verify shared knowledge integrity while not retrieving the whole file. Additionally, is ready to perform multiple auditing tasks at the same time rather than corroborative them one by one. In this scheme Ring signatures is utilized to construct homomorphic authenticators so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. But this scheme unable to handle 1. Traceability-which means the ability of the group manager to reveal the identity of the signer based on verification metadata in some special situations. 2. How to prove data freshness.

Tina Esther Trueman et al [2] Ensuring privacy and data freshness for public auditing of Shared data in cloud” It uses a novel methodology for making certain privacy and data freshness of shared knowledge in cloud exploitation Holomorphic authenticable ring signature (HARS) theme to preserve the user privacy and Overlay tree rule is employed for making certain that users the information with needed level of freshness. Also, Third Party Auditor (TPA) audits the information keep within the cloud. He should be able to verify the trustiness of the CSP while not disclosing the identity of the users within the group. The disadvantage is malicious activities made by means of the user cannot be detected. The hassle with this system is to extend the traceability, which means only the authentic user, can monitor the identity of the signer in order to preserve the malicious pastime made via the user within the group.

Rongxing Lu et al [3] Toward Efficient and Privacy-Preserving Computing in Big Data Era Introduced an efficient and privacy-preserving cosine similarity (PCSC) computing protocol in reaction to the efficiency and privacy requirements of data mining in the Big data era. The proposed PCSC protocol isn’t only privacy maintaining however also efficient. It is particularly appropriate for big data analytics. The gain is the computation overhead of the proposed PCSC protocol also will increase when n is large. The downside is needs to provide specific privateness for some specific big data analytics. Introducing protocol like privateness computing to provide whole and unique protection in Big Data era.

S. Fugkeaw et al [4] Privacy-preserving access control model for big data Cloud”: Propose a singular access manage model combining Role-primarily based Access Control (RBAC) version, symmetric encryption, and cipher text attribute-based totally encryption (CP-ABE) to aid fine-grained access control for big facts outsourced in cloud storage systems. We also reveal the efficiency and overall performance of our proposed scheme through the implementation.

J. Yu et al [5]: Enabling Cloud Storage Auditing with Verifiable Out-sourcing of Key Updates.”: On this paradigm, key updates are frequently accurately outsourced to a few authorized parties, and as a result the important thing-update burden at the patron are going to be kept minimal. The third-party auditor (TPA) in many present public auditing designs, permit it play the function of legal celebration in our case, and make it in Rate of each the storage auditing and therefore the relaxed key updates for Key-exposure resistance. In this technique, TPA simplest ought to maintain an Encrypted model of the client’s secret key at the same time as doing of these burdensome obligations on behalf of the client. The consumer simplest must download the encrypted mystery key from the TPA while uploading new files to cloud. Except, this layout additionally equips the consumer with functionality to further verify the validity of the encrypted mystery keys supplied by using the TPA. one hassle with this system is that the TPA have to perform the outsourcing computations for key updates under the situation that the TPA doesn’t understand the important secret key of the patron.

Tejaswani et al. [6] has proposed a privacy preserving public verifiability for integrity of data storage in cloud using Merkle hash tree whereas the confidentiality of data is achieved using RSA based cryptography algorithm. In this proposed method, user first generates public and private key and then encrypt the file along with computing signature over the encrypted file. User sent the signature and public key to TPA. After that TPA creates a task and sent to the server. Server computes comeback and provides it to TPA. Later TPA checks the integrity of data comparing response with signature. The proposed approach is secure. Also, integrity and confidentiality of data is achieved. It does not support data dynamics along with batch auditing.Yuan et al. [7], a single cloud node is used to keep track of validation tag which was last updated by the rescinded users. In this situation, if the cloud node answerable for tag update is negotiated due to some inside faults or outdoor attacks, the revoked user will be able to produce legal validation tags gain.

Wang et al. [8] has also proposed a design that permits the users to examine the data stored in the cloud storage. This technique may useful to detect the modified blocks simply using homomorphic token pre-computation technique and then erasure coded method is used to get the chosen blocks from multiple servers. To accomplish data storage correctness and data error localization at the same time, it makes use of precompiled verification tokens.

He et al. [9] proposed a scheme in which data owner encrypts the information file first by using renewing code and then coded file will get stored transversely on multiple cloud servers. Multiple cloud servers may suggest similar service provider or different service providers. Data owner may perform a block-level dynamic operation on the outsourced data as block modification, insertion, and deletion. Auditor could cleverly authenticate integrity of data stored on multiple cloud servers; again, data file is frequently modernized by data owner. The secrecy and honesty of data stored in cloud are the reputation perceptions in cloud computing.

More et al. [10] has proposed a mechanism using a MHT and RSA algorithm. In their system, she has implemented a system which provides a public auditability for static data only. If the owner makes some changes in original file then TPA fails to give the appropriate result. Again, it fails to provide batch auditing.

III. DESIGN ISSUES

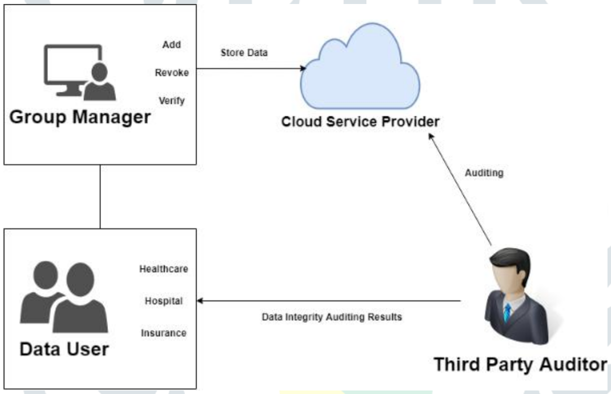

Fig. 1. Proposed System Architecture

As shown in Fig. 1, there are three entities, which are the cloud storage server, users and a Third-Party Auditor (TPA) in our cloud storage model. The cloud storage server provides remote data storage services for the user. TPA, which can be anyone in the system, checks the data storage integrity of client outsourced database. The users, including patients, clinic, hospital, medicine center, insurance, etc., are able to outsource large databases to the server. Unlike most auditing schemes, the client generates the aggregated authentication tags locally and sends them to the cloud. Then, the user could query and update the database and check the data storage integrity. The TPA could check the data storage integrity of the frequently updated database using public key in an efficient way.

In our dynamic group member scenario, any group user can upload own database to the cloud and share them with other group members. And a trusted group manager is responsible for joining or revoking on a user.

A. Algorithms

1. AES Algorithms

1) Input:
2)128 bit /192 bit/256 bit input (0 , 1)
3) Secret key (128 bit) + plain text (128 bit).
4) Process:
5)10/12/14-rounds for-128 bit /192 bit/256 bit input
6) Xor state block (i/p)
7) Final round: 10, 12, 14
8) Each round consists: sub byte, shift byte, mix columns, add round key.
9) Output:
10) Cipher text (128 bit)

2. MD5 (Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Steps:

1. A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
2. The output of a message digest is considered as a digital signature of the input data.
3. MD5 is a message digest algorithm producing 128 bits of data.
4. It uses constants derived to trigonometric Sine function.
5. It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
6. Most modern programming languages provides MD5 algorithm as built-in functions.

B. Mathematical Model

Let us consider S as a system for EHR Sharing System .

S=

INPUT:

Identify the inputs

F= f1, f2, f3 ....., FN— F as set of functions to execute commands.

I= i1, i2, i3—I sets of inputs to the function set

O= o1, o2, o3.—O Set of outputs from the function sets, S=I, F, O

I = Patient records uploaded by the user O = Output i.e. Security

F = Functions implemented to get the output.

Space Complexity:

The space complexity depends on Presentation and visualization of discovered patterns.

More the storage of data more is the space complexity.

Time Complexity:

Check No. of patterns available in the datasets= n

If (n(1)) then retrieving of information can be time consuming.

So the time complexity of this algorithm is O (nˆn).

= Failures and Success conditions. Failures:

1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure. Success:

1. Search the required information from available in Datasets.
2. User gets result very fast according to their needs.

IV. Results and Analysis

In this subsection, our System evaluate the performance of the proposed scheme by several experiments. System run these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the many type of encryption algorithms such as AES Algorithms. In our experiments, System first Install required Software.

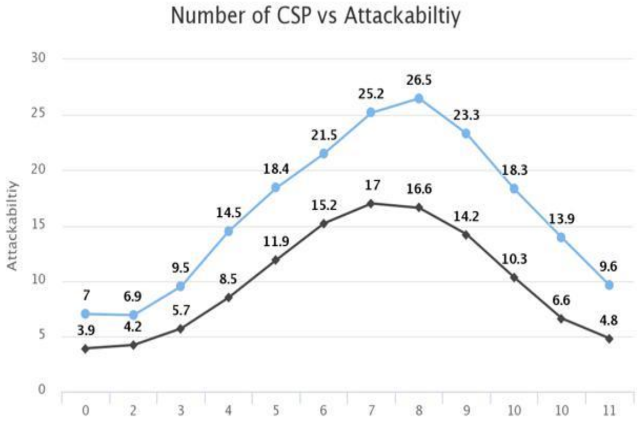

Fig. 2. Graph Between Number of Cloud service provider vs attacker

V. 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.

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] V. 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 Shar-ing 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 Au-ditability 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