|| Volume 3 || Issue 9 || September 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A Survey on Identity-Based Integrity Auditing and Data sharing with Sensitive Information Hiding For Secure Cloud Storage

Sneha D. Raut[1], Mr. Nagaraju Bogiri[2]
Dept. of Computer Engineering K.J. College of Engineering and Management Research,Pune[1 2]
Sneha.raut320@gmail.com[1], mail2nagaraju@gmail.com[2]

Abstract— **Now a day's cloud storage is used for the storage of large data and it provides storage platform for enterprise and individuals and also using cloud storage system user can store and access data remotely. It is avoiding committee of a large number of users for the managing and purchasing software and hardware. In cloud storage auditing key exposure is the one of security problems. In commonly used cloud storage system Electronic Health Records (EHR) it contains the sensitive information and this sensitive information can be exposed when cloud files are shared. Using the encryption techniques, sharing files is hiding from the other users. Addressing such type of problems we propose remote data integrity auditing techniques this system can hide sensitive information when data sharing in the cloud. For this, here we use a sanitized for sanitize data blocks which are regarded to the sensitive information of the files and after that it transfers these block signatures into valid ones for sanitized files. Signatures are used for verifying integrity of the sanitized file in phase of integrity auditing. These techniques are able to secure file storing and sharing on the cloud and also it hide sensitive information. This technique based on the Identity Based Cryptography.**

Keywords: Electronic Health Record, Sanitizer, Cloud Storage, Sensitive Information and Data Sharing.

I INTRODUCTION

With the large amount of data, it is burdened on users to store data locally. Thousands of organizations and individuals want to store data on the cloud. The data store on the cloud is corrupted or lost because of the Hardware fault, human error and software bug in the Cloud. So for verifying whether the data is secure and correctly stored in the cloud, proposed a several data integrity auditing schemes [1].

Cloud storage does trigger some new security threats to data owners. A number of cloud users would not like to use cloud storage due to some serious security worries. A primary concern of cloud users is the integrity of their outsourced files. There are a few factors that might lead to data corruption. First, cloud service providers are not fully trusted. As a result, for monetary reason, the cloud service provider might delete the data that are rare or have not been accessed so that it can save the space for storing other files for charging extra expenses. Second, the stored data could be corrupted due to cloud server failure, management errors or adversary attacks. However, in order to maintain a good reputation, a cloud service provider may deliberately hide data loss events. In cloud storage, data integrity and leakage have become a primary concern of cloud users [2].

In remote data integrity auditing schemes for data blocks, data owner need to generate signatures before uploading data in the cloud. The cloud is processed these blocks. It proves by using signature in the phase of integrity auditing. After that the data owner uploads their data along with signature in the cloud [3].The cloud stored data shared with multiple users in many cloud storage applications, like a cloud, google drive and Dropbox. Data sharing is the main and important feature in cloud storage. Using this feature user shares their data with others. The stored data on cloud contain some sensitive information. The Electronic Health Records (EHRs) contain patient sensitive information and hospital sensitive information. This data stored and shared on a cloud. If this HER data directly uploaded on cloud for research purpose, the sensitive information is exposed to the cloud. Because of the human error, hardware and software failure, the integrity of the EHRs needs to be guaranty. Remote data integrity protected the data with sensitive information [4].

A solution to this problem is to encrypt files before uploading in cloud and after that generate a signature for verifying the integrity of this encrypted file. Then upload this encrypted file along with its signature to the cloud. This method can only show hidden sensitive information. The encrypted file decrypt only by the data owner. Due to this the shared file does not used by others. The possible solution to this problem is to distribute the decryption key to the researchers. This method is not feasible in real scenarios. Firstly, for distributing decryption key to need secure channel [5].It's very confusing to know which researchers will use his/her EHRs in the near future when he/she uploads the EHRs to the cloud. Encrypting the whole shared file for hiding sensitive information, as a result it's impractical. Thus, how to realize data sharing with sensitive information hiding in remote data integrity auditing is very important and valuable. Unfortunately, this problem has remained unexplored in previous researches [6] [7].

II AN ILLUSTRATIVE EXAMPLE FOR EHRs

Here to discuss about the EHR (Electronic Health Records). Figure 1 shows the example of the EHR (Electronic Health Records).

In these EHRs contains data with sensitive information in two parts. One is personal and second is organizational sensitive information. Patient sensitive information includes patient name, ID number and organizational sensitive information such as hospital name. Generally, the sensitive

information is replaced when HER data is uploaded in cloud for research purpose. For the EHR information system in a hospital, the sanitizer work as system administrator. To the sanitizer personal sensitive information should not be exposed. And all information hasn't exposed to the cloud and users.EHRs of patient's data is generated by doctor and send to the sanitizer for storing in the EHR information system. However, these EHRs usually contain the sensitive information of patient and hospital, such as patient's name, patient's ID number and hospital's name.

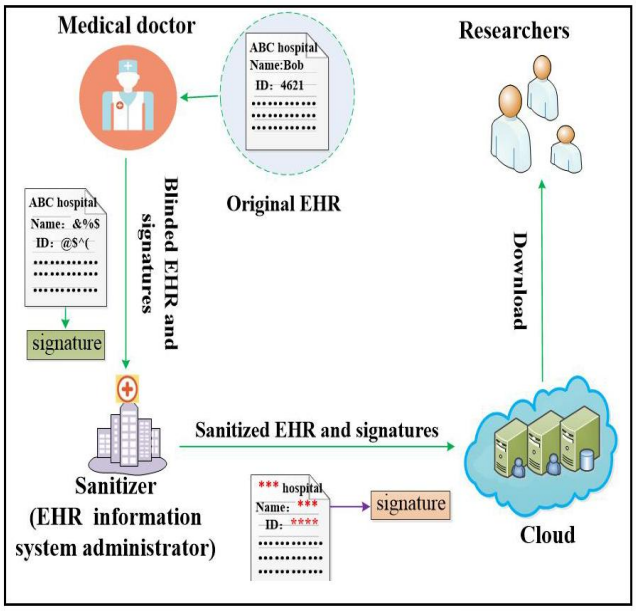

Figure 1: EHRs Example

To preserve the privacy of patient from the sanitizer, the medical doctor will blind the patient's sensitive information of each EHR before sending this EHR to the sanitizer. After that medical doctor generate signature for blinded EHR and sends them to the sanitizer. This message sanitizer stored into the EHR information system. Medical doctor send request to the sanitizer when it requires HER. And then from the EHR information system sanitizer downloads the blinded EHR and sends it to the medical doctor.

Finally a medical doctor recover the original information form blind EHR. When this EHR needs to be uploaded and shared in the cloud for research purpose, in order to unify the format, the sanitizer needs to sanitize the data blocks corresponding to the patient's sensitive information of the EHR. To protect the data, the sanitizer needs to sanitize the data blocks. Data block signatures are transformed by sanitizer into a valid one for the sanitized EHR. Using this remote data integrity auditing is able to perform effectively. At the time of sanitization process, the sanitizer not needs to interact with the medical doctor. Then finally sanitizer uploads these sanitized with respective signature to the cloud. This way, the EHR information can be shared and used for research purpose, when the sensitive information is hidden. The sanitizer is important because of the following reasons. First are the data blocks within the related patient, sensitive information is blinded. The content of this data blocks is very messy code. The sanitizer used format to change the content of the data blocks. Second, the sanitizer can facilitate the information management. The sanitizer sanitizes the EHR and then uploads these sanitized EHR on the cloud at fixed time. Third is when a medical doctor need to EHR it send request to sanitizer as an administrator of EHR information system, then sanitizer download the blinded EHR from the EHR information system and sends it to the medical doctor. This way a medical doctor recovers the original EHR from the blind EHR.

III LITERATURE SURVEY

WentingShen, Jing Qin, Jia Yu, RongHao, and Jiankun Hu[1], Now a day's cloud storage is used for the storage of large data and it provides storage platform for enterprise and individuals and also using cloud storage system user can store and access data remotely.It is avoiding committee of a large number of users for the managing and purchasing software and hardware. In cloud storage auditing key exposure is the one of security problems. In commonly used cloud storage system Electronic Health Records (EHR) it contains the sensitive information and this sensitive information can be exposed when cloud files are shared. Using the encryption techniques, sharing files is hiding from the other users.

J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong [2], a paper discussed about the identity-based signatures. In this paper proposes an intrusion-resilient identity-based signature (IRIBS) method. In this method refresh the secret key using homomorphic structure in key update. It also provides the solution for construction for IRIBS schemes.

J. Yu and H. Wang [3], Key security is one of the critical problems with cloud storage auditing. In this paper author develops a strong key-exposure resilient auditing for secure cloud storage. They define the definition and the security model of this new kind of cloud storage auditing.

G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min [4], in this paper author define the ID-based RDIC and its security model. It also includes the security against cloud server and privacy against a third party verifier.ID-based RDIC protocol does not leak the information of stored data at the time of verification of RDIC process. The result shows that it's secure against server in the generic group model. The proposed model is very secure.

A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang [5],the author discussed about the cloud services. Cloud storage can be easily modify and share. In this paper proposes a privacy-aware public auditing mechanism. This mechanism is proposed for share data. In this mechanism one t group manager for recovering the key and it eliminate the abuse of single-authority power and provides nonframeability. It also traces the data changes. When the current data block is damaged it recovers the correct data blocks. The proposed mechanism is secure and efficient.

Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren [6], in this paper propose a storage auditing scheme. Using this scheme to achieve highly efficient user revocation independent of the total number of file blocks and it possessed by the revoked user in the cloud. This is achieved for key generation and a new private key update technique. When the authenticators are not updated, the integrity auditing of the revoked user's data can still be correctly performed.

IV CONCLUSION

In this paper discussed about the Identity-Based data integrity auditing mechanism for secure cloud storage, which supports data sharing with sensitive information hiding. In this techniques file stored in the cloud can be shared and used by others on the condition that the sensitive information about the file is protected. Proposed mechanism can be achieves desirable security and efficiency.

REFERANCES

[1]WentingShen, Jing Qin, Jia Yu, RongHao, and Jiankun Hu, "Enabling Identity-Based Integrity Auditing and DataSharing with Sensitive Information Hiding forSecure Cloud Storage", 2018.

[2] J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction," 2018.

[3]J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," 2017.

[4]G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," 2017.

[5] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," 2017.

[6] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data", 2018.

[7] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacy preserving authenticators for cloud storage," 2017.

[8] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K. K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," 2017.

[9] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," 2017.

[10]Haiyang Yu, Yongquan Cai1, Shanshan Kong, ZhenhuNing, FeiXue and Han Zhong, "Efficient and Secure Identity-Based Public Auditing for Dynamic Outsourced Data with Proxy.", 2017.