International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

# Data Sharing using Searchable and Auditable ABE with Sensitive Detail Masking Technique

**Prof. R. V. Mante, Nikhil R. Bajad**
Department of Computer Science and Engineering, Government College of Engineering, Amravati, Amravati, India

## ABSTRACT

In cloud storage services, data is being stored on the cloud by user and can be shared by others. Electronic health records system is one of the common system for cloud storage. The cloud file may include sensitive data, that data should not be revealed by others. Encrypting whole shared file may secure the data but makes that data unshared by other users. Users time and memory is saved by storing data in cloud, but once user stores data in cloud he loses control over his data. So the system is proposed having third party auditor for safe and easy use by the users. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file. Meanwhile, the proposed scheme is based on Attribute based Encryption, which simplifies the complicated certificate management. The analysis and the performance evaluation show that the proposed scheme is secure and efficient.

**Keywords :** Cloud storage, data sharing, sensitive information hiding, Attribute-based encryption, multi-keyword search, public auditability.

## I. INTRODUCTION

Cloud computing is the technology of using remote services via internet. In this proper on demand access is provided for shared resources like servers, networks, applications and storage. Scalability, availability and agility of data is improved by use of cloud. It offers users as well as many organizations to place huge amount of data in the cloud. But because of security threats still several users hesitate to store the data in cloud. Data breaks might get hidden by some service providers in cloud to protect their status, might free the space by some providers by erasing less recovered or inactive data. In cloud, across the distributed network the data can be placed anywhere in any one of the data server. The nature of cloud hikes a serious concern about the integrity and privacy of user's data. To safeguard the privacy and integrity of cloud data the auditing approaches and concept of cryptography are used.

Hashing is a method of taking a large block of data and reducing it to reduced blocks of data in a detailed order by using hashing functions. Hashing is used to authenticate the integrity of the content by identifying all modifications and thereafter changes to a hash output. In this scheme multi-keyword can be explored and the search privacy is protected, which can greatly improve the accuracy of keyword search. For instance, the Electronic Health Records (EHRs) stored and shared in the cloud usually contain patients' sensitive information (patient's name, telephone number and ID number, etc.) and the hospital's sensitive information (hospital's name, etc.). The sensitive information of patient and hospital will be certainly exposed to the cloud as well as researchers, if

the EHRs are directly uploaded on cloud to be shared for research goals.

Auditing is the effective method to check the data integrity on cloud. It is the process of validating client's data performed by the client or through the Third Party Auditor(TPA). TPA is the one who audits data of cloud user and has more skills and abilities than users. TPA excludes the involvement of client in auditing process. This nature of TPA creates less burden on users and management of data will be easier to them. There are most of attribute-based encryption (ABE) schemes that are existing and at user client computational costs are high. These problems greatly limit the applications of ABE schemes in practice. To solve the problems of network bandwidth waste and high computational cost, a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme is scheduled for cloud storage, and many computing tasks are outsourced to cloud proxy server to reduce local computing burden, in this scheme the verification of exactness of outsourced private keys is also supported.

## II. LITERATURE SURVEY

In order to check the integrity of information stored in cloud, many remote information integrity auditing patterns have been proposed. To decrease the computation load on the user side, TPA is presented to periodically authenticate the integrity of data on cloud on behalf of user.

[1] Consist of scheme that is data integrity auditing that actualizes data sharing along with sensitive information being hidden is proposed. In [2] proposed an idea of Provable Data Possession for ensuring the data control at untrusted cloud. In this scheme to attain blockless authenticating and reduce I/O costs, homomorphic authenticators and random sampling approaches are used. [3] defined a model Proof of Retrievability and also proposed a scheme. In this, the data stored over a cloud can be recovered and also the integrity of this data can be guaranteed. [4] In this paper, multi-keyword can be searched and also the search privacy is protected. In this proposed scheme, multiple computing processes are outsourced to the cloud proxy server, which highly decreases the computing load at user client.

In [5] If the cloud storage is local users should able to use it, without troubling about the necessity to authenticate its integrity. Thus, enabling ability for public auditing to cloud storage is very importance so that for checking the integrity of data which is outsourced users can retreat to TPA.[6] exploited a different arbitrary masking technique to supplementary paradigm a remote information integrity auditing scheme supporting data confidentiality protection. This pattern achieve better efficiency equated with the scheme in [5]. [7] Introduced Third Party Medium to project light-weight remote information integrity auditing pattern. In this pattern, it helps user to create signatures on the circumstance that the data privacy can be safe. To decrease the computation load of signature generation for user side, [8] designed a remote data integrity auditing scheme based on the indistinguishability complication technique. [9] constructed a shared data integrity auditing scheme supporting user revocation. The aforementioned schemes all rely on Public Key Infrastructure, which incurs the considerable overheads from complicated certificate management. [10] The works on assuring remote data integrity require support of either dynamic data operations or public auditability, this paper fulfil both. For supporting data dynamics, [11] firstly projected a partially dynamic pattern. [12] used a skip list to create a fully data dynamic auditing pattern.

In [13] and [14], and [15] If the secret key used for auditing is been unprotected, most of the present auditing protocols would definitely become unable to work. In this scheme, new aspect of auditing with

cloud storage is being focused. The way is investigated to decrease the damage of client's key exposure in the cloud storage auditing, as well as to get the first practical solution for the new problem setting. The definition and the security model of auditing protocol with key-exposure flexibility is assigned and propose such a protocol. In system design, to renew the secret keys for client the binary tree structure and the pre-order traversal technique is used. To support the perfect forward security and property of blockless verifiability a novel authenticator construction is developed [16]. The information sharing is an essential application in cloud storage scenarios.

[17] created an well-organized shared data integrity auditing scheme, which not only supports the identity privacy but also attain the distinctiveness traceability of users. To safeguard the identity privacy of user, [18] considered a privacy-preserving shared data integrity auditing scheme by adapting the ring signature for secure cloud storage. [19] proposed a shared data integrity auditing scheme by user revocation by using the proxy re-signature. With the employment of the Shamir secret sharing technique. [20] planned a privacy-aware shared data integrity auditing system by manipulating a homomorphic provable group signature. In order to support efficient user revocation.

## III. PROPOSED METHODOLOGY

Components used in the system are:

- Data Owner: The data owner stores the data which are for record purpose or for any personal use. The data file is being store by owner on the cloud after being data sanitizing and hashing of the data.
- PKG: The PKG is trusted by other entities. It is responsible for generating system public parameters and the private key for the data owner to store the data.
- Sanitizer: Data Sanitization is part of a comprehensive, best practice security policy. So sanitizer is used in the proposed system so that the data blocks are stored on cloud after being sanitized as the data owner sends that particular file for the further process.
- Cloud: The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to cloud and share that data with others.

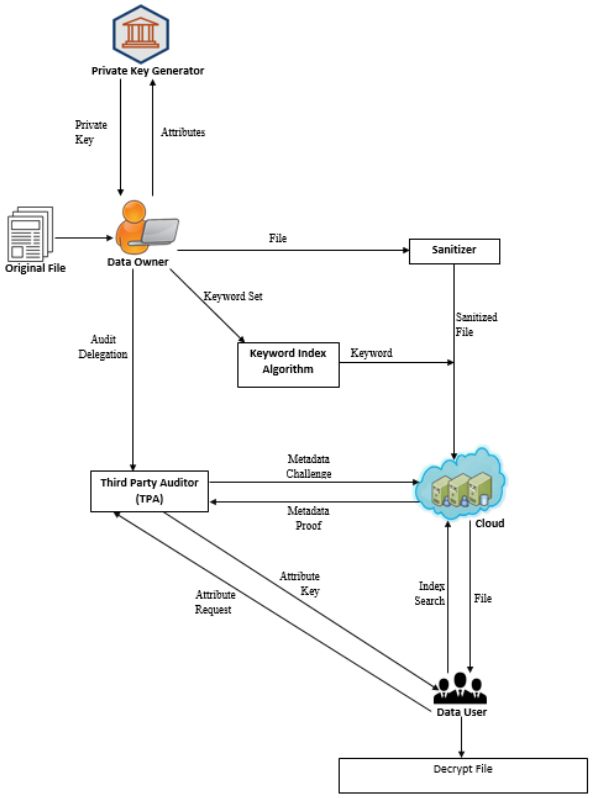


**Figure 1** : Proposed System

- User: In this scheme users are being attached with cloud but depends on the Third party auditor. Users firstly takes the attribute key by requesting it to TPA and then that key helps user to get data from cloud.
- TPA: The TPA is a public verifier. It is being used in the proposed system in which the user will easily get the attribute key and so that user can get data with the help of it. It is in charge of verifying the reliability of data kept in the cloud representing users.

- Attribute based encryption is a public key encryption which consists the secret key of a user and the cipher text and that are dependent upon attributes (e.g. the region in which they live, or the kind of category they belong to. In this structure, attribute key is stored in the third party auditor. When user request with the attribute and if they got match then the attribute key is given to user by TPA and then user can get data from cloud.
- Hashing is used to confirm the integrity of content by perceiving all modifications and after that changes to a hash output. Encryption encodes data for the leading purpose of maintaining data confidentiality and security. Proposed work is as follows:

### A. Providing Data Confidentiality

The data owner or clients asks the cloud server to provide service. The cloud server authenticates the user by his particular username and password. Also the user must authenticate cloud server with his username name and password. After authentication, the data owner will select the file to upload to cloud. Before uploading the file to cloud, the data owner divides the data file in to blocks. The file blocks are then encrypted with ABE algorithm and later generates the message digest (Metadata) for the file using SHA algorithm. The encrypted file is uploaded to cloud. Note that the data in cloud is stored in encrypted form and hence achieves data confidentiality.

### B. Providing Data Privacy

Data privacy means, the third party auditor should have no idea of owners data. In other words, TPA should audit files without having knowledge about user's actual data. As stated previously, the blocks of data file are encrypted using ABE and tailed by computing hash function or message digest using SHA Algorithm. This message digest is given to TPA and TPA will use this digest to prove integrity of data during verification process. Note that, the data file of data owner is given to TPA in form of metadata. Thus, TPA will not come to know about owners actual data, achieving owners data privacy.

### C. Sensitive information hiding

To ensure that the personal sensitive information of the file is not exposed to the sanitizer, and all of the sensitive information of the file is not exposed to cloud and shared users. In our scheme multi-keyword can be searched, and the search privacy is protected. Most of the computational burden is out-sourced to cloud proxy server to reduce local computing task at user client, including private key generation, encryption, and decryption algorithm. Also supports the verification of outsourced private keys. The security of this scheme is proved that under the adaptable keyword attacks keyword index is equivalent, and also the cipher text is a particular security over chosen plaintext attacks in the oracle model.

### D. Achieving Data Integrity

Data Integrity means, alteration to cloud data should be detected. In the proposed work, TPA is used to accomplish the auditing process that verifies data integrity. Data owner sends request to TPA to perform data audit of files stored in cloud. Once the TPA gets requests from clients, TPA generates challenge request to the cloud server demanding for the required data that is stored in cloud. Once TPA gets response from cloud server, TPA will start the process of data verification. TPA computes message digest for the file received from cloud using the same SHA Algorithm. In verification process, TPA matches the message digest that was calculated for the data received from cloud with the message digest saved earlier which was sent by client. If two message digests being match, then it directs that stored data is secure and it is not altered by malicious users. If the values doesn't match, it indicates that data is altered by malicious users and data is not secure. After the completion of verification process, TPA directs the results of auditing to the data owner signifying the current status of file. The cloud entity performs two important tasks. Firstly, cloud

stores data in the encrypted from that are uploaded by the cloud users. Secondly, cloud gives response to the TPA's challenge request in the form of replying encrypted data of file that is required to audit. In our proposed method, cloud users can transmit data to cloud storage and can trust TPA to authenticate the truthfulness of data kept in cloud server.

## IV. RESULTS

The result shows the overall performance of the system for Searchable ABE Data Sharing With Sensitive Information Hiding And Public Auditing. The graph for the parameters Encryption, decryption and hash time are shown below

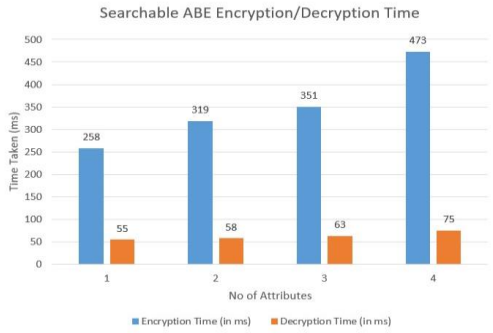


**Figure 2:** Encryption and Decryption time

In figure 2, Encryption and decryption time is given as per the attribute , this figure shows the variation in time with respect to attributes as the no. of attributes increases the time taken for the process also increases particularly.

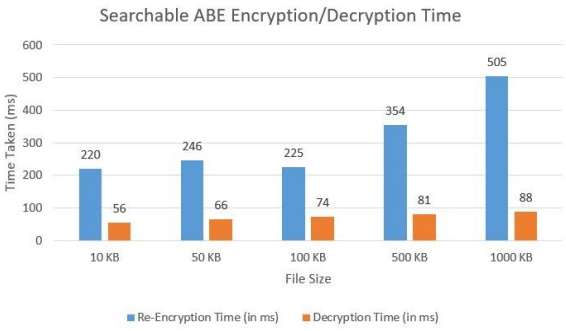


**Figure 3:** Encryption and Decryption time

In figure 3, Encryption and decryption time is given as per the size of file , this figure shows the variation in time with respect to size as the size of file is more the time taken for the process also increases particularly.

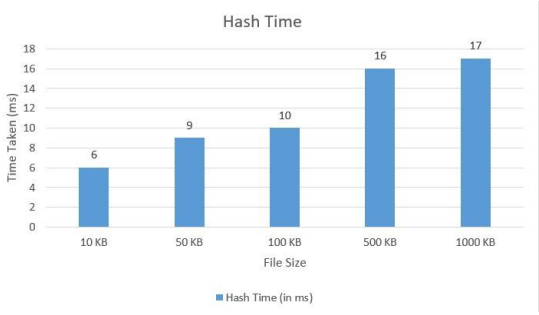


**Figure 3** : Hash Time

In figure 3, Hash time is given as per the size of file , this figure shows the variation in time with respect to size as the size of file is more the time taken for the process also increases particularly.

## V. CONCLUSION

In this scheme various methods and approaches for security of data in cloud and hiding sensitive information is studied. Also, various challenges faced while using or applying the techniques, So Secure data access as well as data share is provided with Attribute based Encryption technique along with Searching facility. Third party auditor and Hashing makes system scalable and reliable, and is used for faster audit generation and verification. Also sensitive information is been hidden, and the results also shows that the proposed system is efficient and effective for storage of cloud data.

## REFERENCES

[1] Wenting Shen, Jing Qin, Jia Yu , Rong Hao, and Jiankun Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, february 2019

[2] G. Ateniese , "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[3] B. S. Kaliski, Jr. A. and Juels, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[4] Shangping Wang , Shasha Jia , And Yaling Zhang , "Verifiable and multi-keyword searchable attribute-based encryption scheme for cloud storage," volume 7, 2019 received March 25, 2019, accepted April 9, 2019, date of publication April 12, 2019, date of current version April 25, 2019.Digital Object Identifier 10.1109/ACCESS.2019.2910828

[5] S. S. M. Chow, C. Wang, K. Ren, W. Lou, and Q. Wang, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[6] C. Xu, S. G. Worku , X. He, and J. Zhao, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, 2014.

[7] J. Yu, H. Xia, X. Lu, W. Shen, R. Hao and H. Zhang, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.

[8] K. Ren, C. Guan, F. Zhang, J. Yu, and F. Kerschbaum, "Symmetric key based proofs of retrievability supporting public verification," in Computer Security—ESORICS. Cham, Switzerland: Springer, 2015, pp. 203–223.

[9] D. Wang, Y. Luo, S. Fu, J. Deng and M. Xu, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2015, pp. 434–442.

[10] C. Wang, Q. Wang, K. Ren, J. Li and W. Lou, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no.5, pp. 847–859, May 2011.

[11] A. Kupcu, C. Erway, R. Tamassia, and C. Papamanthou, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secure., 2009, pp. 213–222.

[12] R. D. Pietro, G. Ateniese, G. Tsudik, and L. V. Mancini, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. no. 9.

[13] K. Ren, J. Yu, V. Varadharajan, and C. Wang, "Enabling cloud storage auditing with key exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.

[14] J. Yu, C. Wang and K. Ren, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.

[15] H. Wang and J. Yu, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.

[16] J. Yu, R. Hao, H. Xia, H. Zhang and X. Cheng, "Intrusion resilient identity-based signatures: Concrete scheme in the standard model and generic construction," Inf. Sci., vols. 442–443, pp. 158–172, May 2018.

[17] J. Yu, G. Yang, Z. Fu, R. Hao and W. Shen, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016.

[18] B. Wang, H. Li and B. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. IEEE 5th Int. Conf. Cloud Comput. (CLOUD), Jun. 2012, pp. 295–302.

[19] B. Wang, H. Li and B. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

[20] S. Yu, A. Fu, Y. Zhang, C. Huang and H. Wang, "NPP: A new privacy-aware public auditing

scheme for cloud data sharing with group users," IEEE Trans. Big Data, to be published, doi: 10.1109/TBDATA.2017.2701347.

[21] 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," IEEE Trans. Depend. Sec. Comput., to be published, doi: 10.1109/TDSC.2017.2662216.

[22] H. Wang, "Proxy provable data possession in public clouds," IEEE Trans. Serv. Comput., vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.

[23] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[24] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptol., vol. 26, no. 3, pp. 442–483, Jul. 2013.

**Cite this article as :**

Prof. R. V. Mante, Nikhil R. Bajad, "Data Sharing using Searchable and Auditable ABE with sensitive detail masking technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 2, pp.336-342, March-April-2020.

Journal URL : http://ijsrcseit.com/CSEIT2062169