International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Secure Cloud Storage based on integrity Auditing and Data sharing with Sensitive Information Hiding

Ms. Magar Surekha V.[1], Mr. Avhad G.T.[2],

[1]Student, Vishwabharati Academy's College of Engineering, Ahmednagar Maharashtra,India
[2]Asst.Prof., Vishwabharati Academy's College of Engineering, Ahmednagar Maharashtra,India

---

Abstract - Now a days cloud storage is used to store big data and provide a storage platform for businesses and individuals and also with cloud storage system user can store and access data remotely. It avoids the commission of a large number of users to manage and purchase software and hardware. In cloud storage, key disclosure is one of the security issues. In a commonly used cloud storage system, Electronic Health Records (EHR), Military information contains sensitive information, and this sensitive information can be exposed when sharing cloud files. Using encryption techniques, file sharing is hidden from other users. To solve this type of problem, we propose remote data integrity auditing techniques; this system can hide sensitive information when sharing data in the cloud. To do this here, we use sanitized to sanitize data blocks that are considered sensitive file information and then convert those block signatures to valid ones for sanitized files. Signatures are used to verify the integrity of the sanitized file in the integrity audit phase. These techniques are able to secure cloud file storage and sharing as well as hide sensitive information. This technique is based on Identity Based Cryptography.

KeyWords: Cloud computing, Storage, Data, Hospital Management, Encryption, Remote Data, Sanitizer, identity based.

1. INTRODUCTION

With a large amount of data, it is burdensome for users to store data locally. Thousands of organizations and individuals want to store data in the cloud. Cloud data storage is damaged or lost due to hardware failure, human error, and cloud software failure. Several data integrity auditing schemes have been proposed to verify that data is secure and properly stored in the cloud. Encrypting the entire shared file can realize the hiding of sensitive information, but it will make it impossible for others to use the shared file. How to implement data sharing with sensitive information hidden in remote data integrity auditing has not yet been explored. To solve this problem, we propose a remote data integrity audit scheme that implements data sharing with sensitive information hidden in this document. In this scheme, sanitization is used to sanitize data blocks corresponding to sensitive file information and transforms the signatures of those data blocks into ones valid for the sanitized file.

Cloud storage introduces some new security threats to data owners. Many cloud users would not want to use cloud storage due to serious security concerns. The primary concern of cloud users is the integrity of their outsourced files. There are several factors that can lead to data corruption. First, cloud service providers are not fully trustworthy. As a result, for monetary reasons, the cloud service provider may delete data that is rare or has not been accessed in order to save space for storing additional files for charging additional expenses. Second, stored data could be corrupted due to cloud server failure, management errors, or adversary attacks.

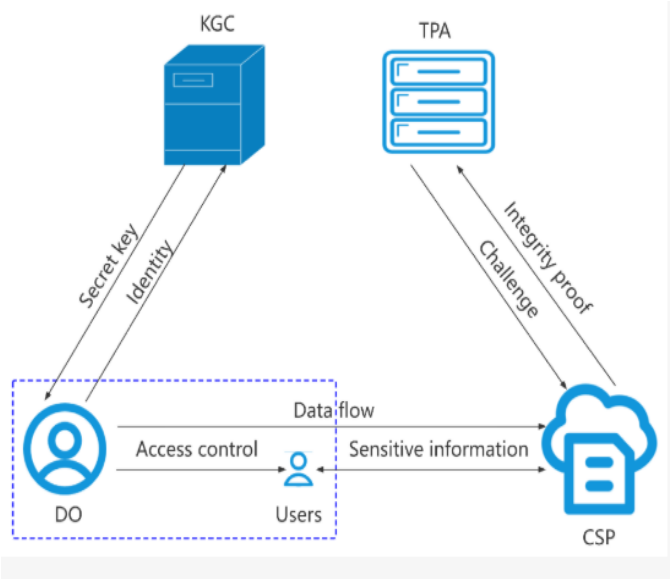

Figure 1. System model.

The objective of the proposed work is to achieve data sharing with sensitive information hidden in remote data integrity auditing and to propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage. In such a system, sensitive information can be protected and other information can be made public. This makes it possible for a file stored in the cloud to be shared and used by others under the condition that sensitive information is protected, while remote data integrity auditing can still be performed effectively. Design a practical identity-based shared data integrity audit scheme with hidden sensitive information for secure cloud storage. Sanitizer sanitizes these blinded data blocks into a uniform format and also sanitizes data blocks corresponding to the organization's sensitive information. It also transforms the matching signatures into valid ones for the sanitized file. This method not only implements remote data integrity auditing, but also supports data sharing under the condition that sensitive information is protected in cloud storage. To the best of our knowledge, this is the first scheme with the above features. In addition, our scheme is based on identity-based cryptography, which simplifies the complex certificate. The result shows that the proposed scheme achieves the desired security and efficiency.

II. RELATED WORK

Lei Zhang et.al [1] author designed a survey on shared data on secure data storage. An effective public auditing solution is used that can simultaneously maintain identity privacy and identity traceability for group members. Specifically, the new cloud data sharing framework is designed for shared cloud data supporting identity privacy and traceability. A group manager is introduced to help members generate authenticators to protect identity privacy, and two lists are used to record members making final edits on each block to achieve identity traceability. In addition, the scheme also achieves data privacy during the generation of authenticators using a blind signature technique.

Cong Wang et.al [2] presented a survey on secure cloud storage: Enabling public auditability of cloud storage is essential so that users can turn to a third-party auditor (TPA) to check the integrity of outsourced data and be worry-free. In order to safely implement an effective TPA, the audit process should not introduce any new vulnerability in user privacy and should not create any additional online burden for users. A secure cloud storage system supporting privacy-preserving public audit is proposed.

J. Yu and H. Wang [3], the author develops strong key exposure resistant auditing for secure cloud storage. key security is one of the critical issues in cloud storage auditing. In this paper, They define the definition and security model of this new kind of cloud storage audit.

Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren [4] propose a repository auditing scheme in this paper. Using this scheme, highly efficient user revocation can be achieved independently of the total number of file blocks the revoked user has in the cloud. This is achieved by key generation and a new private key update technique. If the authenticators are not updated, data integrity auditing of the revoked user can still be performed correctly.

Wei X et.al [5] proposed application scheduling in mobile cloud computing with load balancing. In this paper, a modern web application is designed to help in providing multiple services deployed through complex technologies. Shen W et al. [24] proposed a simple and secure privacy-preserving cloud audit scheme for group users. This scheme helps to reduce the computational load on the user side. Wang B et.al [8] proposed a public audit of shared data with effective user revocation in the cloud, where a third-party auditor is used to store data and provide user authorization.

Shen W et.al [6] conducted a survey on cloud storage auditing. It allows the user to store their

data in the cloud, which ensures high security. Fu A et.al [19] proposed a new privacy-aware public auditing scheme for cloud data sharing with group users. To ensure the integrity of the shared data, a third-party scheme has been proposed. The proposed scheme, a holomorphic true group signature, ensures that a group user can track data changes through a specified binary tree and recover the last correct data block when the current data block is corrupted.

Sundaraj, V et. al [7] proposed an optimized denoising scheme using an opposition-based self-adaptive learning PSO algorithm for a wavelet-based ECG signal denoising algorithm. Since the ECG signal is a very challenging task, many researchers have reported various methods to denoise the ECG signal in the past year. In this paper, an optimized thresholding mechanism for wavelet-based medical signal noise reduction is proposed.

III ALGORITHM USED

Path tracing is a graphical method of plotting routes data navigation taking place in the network so that global illumination is true to reality. This algorithm integrates all data accumulation reaching a single point on the object's surface. This the accumulation is then reduced to sub paths based on different access points at different intervals.

The following items were visualized within this module:

1. Number of total packet reads (in bytes) since the last server start
2. The last packets loaded in a certain interval (Loading data bytes)
3. Number of total enrolment on packages (In number of bytes) since the server was last started
4. The last packets are written at a certain interval (data loading bytes)
5. Connection directed from the last server starts at certain interval (data loading bytes)

IV. THE PROPOSED SYSTEM

Here are considering using this idea in the area of sanitation signature to sanitize sensitive information file by introducing an authorized disinfectant. However that is infeasible if this sanitization signature is used directly remote data integrity audit. First, this signature in is constructed based on chameleon hashes. However, a many chameleon hashes exhibit a key exposure problem. On to avoid this security issue requires the signature used in strongly unforgivable chameleon hashes, which will be inevitable incur huge computational costs. Second, the signature used in does not support blockless verifiability. That means that the verifier must download all data from cloud to verify data integrity, which takes a huge amount communication overhead and excessive authentication time big data storage scenario. Third, the signature used in it is based on PKI, which suffers from complexity certificate management. And then this user will use the designed signature algorithm to generate signatures for a blinded file. If necessary, the user can restore original file from blinded using this blinding factor.

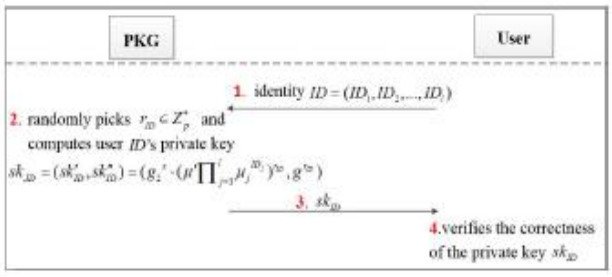

Fig. 2. The process of private key generation

In our proposed scheme, PKG generates a private key for the user by his ID. User can check the correctness of the received private key. When there is a desire for the user to upload the data to the cloud to preserve it personal sensitive information of the original file from sanitizer, this user needs to use a blinding factor to blind data blocks corresponding to sensitive personal information original file.

These signatures will be used to verify the integrity of this blinded file. in addition, the user generates a file tag that is used to secure it file identifier name correctness and some validation values. The user also calculates a transformation value which is used to transform signatures for disinfection. Finally, the user sends the blinded file, its matching signatures, and the file along with the value of transformation into a disinfectant. When the above user messages are valid, disinfection first sanitizes blinded data blocks into a uniform format and also sanitizes data blocks corresponding to organization data blocks sensitive information to protect the privacy of the organization, and then converts their corresponding signatures to valid ones one for the sanitized file using the transform value. Finally, sanitization uploads the sanitized file and the corresponding

signatures to the cloud.

IV. CONCLUSION

In this proposed system an identity-based data integrity auditing scheme is proposed for secure cloud storage, which supports data sharing while hiding sensitive information using steganography. By using stegano-image, it makes systems more secure and provides benefits for applications such as the collaborative world, the government sector, and for personal use. A file stored in the cloud can be shared and used by others as long as the file's sensitive information is protected. In addition, remote data integrity auditing is still possible effectively. The security proof and experimental analysis show that the proposed scheme achieves the desired security and efficiency. In the future, a cloud storage audit protocol with verifiable outsourcing of key updates may be proposed. In this paper, we proposed identity-based data integrity an audit scheme for secure cloud storage that supports data sharing with sensitive information. In our scheme it is a file stored in the cloud can be shared and used by others provided it is sensitive file information protected. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

V REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350

[4] 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.

[5] 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, vol. 22, no. 5, pp. 847–859, May 2011

[6] Wei, X., Fan, J., & Ding, K, “Application scheduling in mobile cloud computing with load balancing”. Journal of Applied Mathematics, 2013.

[7]B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving public auditing for shared data in the cloud,” in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302

[8] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[9] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[10] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[11] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.

[12] J. Hur, D. Koo, Y. Shin, and K. Kang, “Secure data deduplication with dynamic ownership management in cloud storage,” IEEE Trans. on Knowl. and Data Eng.,vol. 28, no. 11, pp. 3113–3125, Nov. 2016.

[13] G. Ateniese, D. H. Chou, B. de Medeiros, and G.Tsudik,“Sanitizable signatures,” Proceedings of the 10th European Conference on Research in Computer Security, ser.ESORICS’05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 159–177.

[14] G. Ateniese and B. de Medeiros, “On the key exposure problem in chameleon hashes,” in Security in Communication Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 165–179.

[15] B. Wang, B. Li, and H. Li, “Panda: Public auditing for shared data with efficient user revocation in the cloud,” IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015.

[16]. H. Shechem, and B. Waters, Compact proofs of retrievability. Proc. of Cryptology-2008, LNCS 5350, pp. 90-107, 2008.

[17]. G. Ateniese, S. Kamara, J. Katz, Proofs of storage from homomorphicidentification protocols. Proc.ASIACRYPT 2009, 319-333

[18]. A. F. Barsoum, M. A. Hasan, Provable multicopy dynamic data possession in cloud

computing systems, IEEE Trans. on Information Forensics and Security, 10(3): 485–497, 2015

[19] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud, IEEE Internet Computing, vol. 16, no. 1, pp.69–73, Jan 2012.