ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

IDENTITY BASED SHARED DATA INTEGRITY VERIFICATION WITH HIDDEN PRIVATE INFORMATION FOR RELIABLE CLOUD STORAGE

[1]N.Pavan, Asst.Prof.,

dept of CSE, Malla Reddy Institute of Technology, Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

[2]Dr. Sateesh Nagavarapu,

Professor, dept of CSE, Malla Reddy Institute of Technology, Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

[3]P. Dhana Sri,

Asst. Prof., dept of CSE, Malla Reddy Institute of Technology, Kompally, Maisammaguda, Dulapally, Secunderabad, 500100

ABSTRACT

Users can remotely store their data into the cloud using cloud storage services and share data with others. To guaranty the credibility of data storages in the cloud, remote data integrity verification scheme is proposed. The cloud storage file might contain some private information in some of the popular cloud storage systems, such as an Electronic Health Records (EHRs). When cloud file is shared, private data should not be accessible to anyone. Encryption of the entire shared file can mask private information, but it will prevent anyone from using this shared file. Data sharing was not investigated with private information concealed in the remote data integrity audit phase till now. A remote data integrity verification scheme is suggested to deal with this problem by exchanging data with others besides hiding private data. A sanitizer is used in this scheme to sanitize data blocks corresponding to the private information files and to convert the signature of those databases to valid data blocks for the sanitized file. Those signatures are used for the integrity check of the sanitized file during the integrity verification process. This scheme thus allows the file that is stored in the cloud to be exchanged and exploited by others subject to the secret privacy of the data and the efficient verification for the remote data integrity. The proposed scheme in the meantime is based on identity cryptography, which simplifies the complicate management of certificates. The safety review and performance assessment demonstrate that the scheme proposed is safe and successful.

Index Terms — Cloud storage; Integrity verification; Data sharing.

1. INTODUCTION

With a huge data growth, data storing locally is a huge burden for the customers. In this way, a rising number of companies and people want their data to be stored in cloud. Data stored in a cloud can nonetheless be defiled or lost because of unavoidable programming glitches, equipment problems and human cloud errors [1]. Many remote data integrity audit plans were submitted to validate if the data is processed in cloud efficiently [2-8]. The data owner has generated data signatures blocks in remote data integrity auditing plans before they are moved to cloud. These signatures are used usually to show that during the time of integrity audit, the cloud truly has data blocks along with their corresponding signatures, the data owner migrated these data to the cloud. Data is available for many cloud storage applications, including Google Drive, Dropbox and iCloud are also spread among many clients. As one of the most regular cloud storage features, data sharing allows different clients to transmit their knowledge to others. However, some private information may be included in these common data placed in the cloud. The private clinic information in the Electronic Health Records (EHRs) [9] stored in the cloud also contain patient private information. If the EHRs are passed to the cloud for research purposes directly, the cloud and the researchers will certainly obtain the private information of the patient and medical clinic.

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

It is, therefore, necessary to conduct remote data integrity audits and the private information is shielded from shared data. It is a possible strategy to deal with this problem by encrypting the whole shared record before it is sent to the cloud, then by finally uploading to the cloud. The signature is used to validate the integrity of this encoded document. This technique will understand the secret private information and only this document can be decrypted by the data owner. It will make difficult for anyone to use the whole shared record. Embedding the patients' EHRs will secure patient and clinic security, but scientists can no longer use these encrypted EHRs. Sending to scientists the decryption key would seem to be a plausible response to the above question. This technique cannot be embraced in actual circumstances for reasons that surround it. First, it requires reliable channels to distribute decryption key that is difficult to accomplish in certain instances. Moreover, when the EHRs is moved to the cloud, it would seem difficult for the consumer to know which researcher would soon use his or her EHRs. So through encryption of the entire common text, it is illogical to conceal private information. This is a significant and important way to recognize the exchange of data with private data concealed in remote audit integrity. This subject has remained unknown in past studies. To examine the exchange of data with private information hiding in the audit of the remote data integrity, an idea for secure cloud storage is proposed, called identity-based data integrity verification using hidden private information. Private information could be assured in such a plan and other information transmitted. It was ready to share and use the document saved in the cloud depending on the condition that privacy is protected.

A. Related Work

Numerous remote data integrity auditing plans have been proposed to confirm the integrity of the data stored in the cloud. Third-Party Auditor (TPA) is aware of the integrity of the cloud data for the good of the customer to reduce the measurement issues on the client-side. Ateniese et al [2], raised a thought to ensure data ownership in the cloud untrustworthy, with Provable Data Possession (PDP). Holomorphic authenticators and irregular inspection systems are used for block less testing and I/O costs in their proposed plot. Juels and Kaliski [3] defined and suggested a realistic strategy for the model, called Proof of Retrievability (PoR). This strategy will retrieve the data entered in the cloud and guarantee the confidentiality of these data. In the light of pseudorandom capability, Shacham & Waters [4] suggested a private data-integrity audit plan and data integrity audit plan, which is far away from the public. Wang et al. [5] introduced a remote data integrity audit framework that would protect data security. Solomon et al. [6] used a remote data integrity auditing random masking technique framework that supports data security. Guan etc al. [7] developed an audit scheme for Integrity of remote data dependent on the methodology of indistinguishability. Shen et al. have introduced a Third-Party Media (TPM) [8] to build a lightweight remote data integrity management framework. Ateniese et al. proposed PDP [10] scheme which was partly a complex one.

Erway et al. [11] used a list of skips to create a completely interactive audit framework with data. A further remote data integrity audit framework was proposed by Wang et al. [12] to support full dynamic dynamics using Merkle Hash Tree. To mitigate the harm of users' key exposures, Yu et al. [13–15] suggested Key-Expose stable frameworks based on key upgrade methods of remote data-integrity auditing [16]. In cloud storage scenarios the data sharing is an essential application. Wang et al. [17] have established a mutual data integrity audit framework to protect the user's identity privacy by changing the ring signature for protected cloud storage. An efficient shared data integrity auditing scheme has been developed by Yang et al. [18] that not only promotes personal Data security achieves traceability of user identity only. Fu et al. [19] have built a framework for the audit of data integrity by using a homomorphic group signature.

Wang et al. [20] introduced a common data integrity audit scheme using the proxy signature in support of efficient operator revocation. Luo et al. [21] have established a standard data integrity audit scheme promoting user revocation, using Shamir's secret sharing technology. All the above schemes depend on Public Key Infrastructure (PKI). The complicated management of the certificate involves significant overhead. Wang et al. [22] suggested an identity-based, multi-cloud-based, remote data integrity audit scheme to simplify certificate management. This software replaces the public key with information about your identities, such as the user name or e-mail address. Wang et al. [23] have built a new remote data integrity management mechanism focused on identity by implementing a proxy to process user data. Yu et al. [24] have established the complete security of data Identity-based encryption mechanisms privacy. Wang et al. [25] suggested a data integrity audit scheme based on an identity that satisfies unconditional privacy and incentive.

2. PROBLEM STATEMENT

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

With the exponential growth of data, storing the sheer volume of data locally is a major burden on users. More and more businesses and people want to store their data in the cloud.

However, some private information could be found in the cloud [26]. A possible solution to this issue is encrypting the entire standard file [27] and then creating signatures to ensure its integrity before it is sent to cloud. This method can mask private data since it can be decrypted only by the data owner. It will however prevent the entire shared file from being used.

3. PROPOSED METHOD

Identity-based shared data integrity verification with hidden private data for reliable cloud storage is proposed. Next, the user blinds the data blocks and submits corresponding signatures to a sanitizer. The sanitizer cleans the blinded data blocks and uploads to the cloud in a standard format. Private information can be guarded and other information can be made available. This means you can share the file saved in the cloud and use it by anyone subject to privacy. We consider using the sanitizable signature [28] to complete the exchange of data with private information to sanitize privacy by adding an authorized sanitizer. In both instances, it is difficult to legally use this sanitizable signature in the verification of remote data integrity. The signature is based on the hash signatures. In any case, the biggest introduction challenge is a lot of chameleons. The verifier must retrieve all data from the cloud to verify the credibility of the data, which cause overhead correspondence and excessive confirmatory time in huge storage conditions. The signature used depends on the Public Key Infrastructure (PKI), another active signature calculation in the signature generation process is used to resolve the above issues. The planned conspiracy labelling provides block less encryption, allowing the verifier to track data integrity without downloading all cloud data.

The Private Key Generator (PKG) produces the private customer key permitting to its character ID in the proposed framework. The customer should verify that the private key is correct. If the customer wishes that data is moved towards the cloud to store the private data from the sanitizer in the first record, the customer has to use an element to blind blocks compared with the personal data in the first text. When necessary the customer can retrieve the first document from the blind by using this blinding component. And then this customer uses the signature algorithm for the blinded paper. These signatures are used to authenticate that this blinded document is integral. Also, the customer creates a document tag that is used to ensure record identifier accuracy. Finally, the customer sends the blinded document, their reference signatures and the record along with the transformation value to sanitizer. The sanitizer ensures that blinded data blocks are sanitized in a uniform configuration and additionally sanitizes the data blocks in comparison with the private information of the association for the security of the association. The sanitizer passes to the cloud the sanitized record and the signatures. The cloud provides an audit confirmation in compliance with the TPA test when the data integrity audit task is performed. If this verification is accurate, the TPA will confirm the integrity of the sanitized record placed away from the cloud.

4. SYSTEM DESIGN

The model involves 5 kinds of different substances: Cloud, Client, Sanitizer, PKG and TPA, as visible in Fig.1. The construction model contains five different types of entities.

(1) Cloud: Cloud provides the client with massive extra storage space. Clients can transfer their data to the cloud and sell their data to others via cloud storage administration.

(2) Client: Client is a member of an organization that has multiple documents to be stored into cloud.

(3) Sanitizer: The Sanitizer shall sterilize the data blocks compared to the private information in the documents and convert the signatures of the data squares into valid ones the cleaned document and shall transmit the sterilized record and its associated signatures to the cloud.

(4) PKG: It is responsible for defining public limits and the private key for the customer in compliance with its identification.

(5) TPA: It is in the interest of consumers to confirm the completeness of the data placed on the cloud.

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

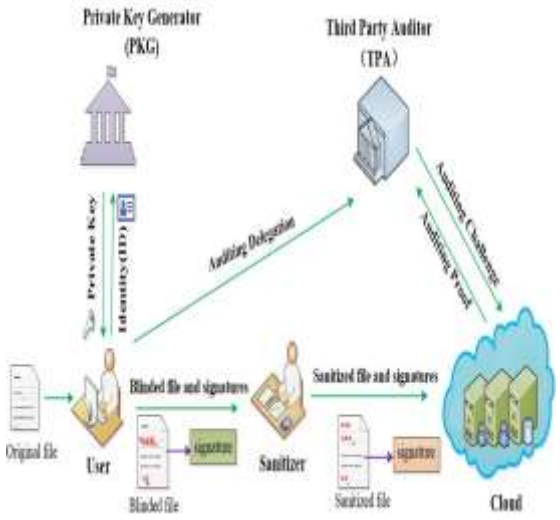

Fig: 1. System Model

5. ALGORITHM IDENTITY-BASED ENCRYPTION

Identity-based encryption is a form of public key encryption where a user gets public key from a trusted Private Key Generator (PKG) and the corresponding private key can be generated from public key. So, there is no need for distributing the keys. In this, the algorithm is further classified into six types such as Setup, Extract, SigGen, Sanitization, ProofGen and ProofVerify.

1)Setup (1k) is a PKG configuration algorithm. A security parameter k is required as an input. The master secret key msk and public device parameters pp are generated.

2) Extract (pp, msk, ID) is run by the PKG. It uses pp, mask's master secret key and user identity ID as input device public parameters. The privately held key skID of the user is produced. The user can check that skID is right and can only recognize it as his private key if the check has been carried out

3) SigGen (F, skID, ssk, name) is user identity. The file F, the private key skid of the user, private key ssk of the user signing and the name of the file identifier is used for the input. The blinded file F*, its respective symbol Φ and the file tag μ are generated.

4) Sanitization (F*, Φ) is the algorithm used by the sanitizer for private information sanitization. The blinded file F* and its signature collection are used as input. The sanitized file F' is output and its respective signature sets are set to **Φ***'*.

5) ProofGen (F', Φ', chal) is the evidence generation cloud algorithm. The file F', the corresponding signature set and the challenge to audit take as input the corresponding signature set. It produces a test P which demonstrates that the cloud has this sanitized F' file.

6) ProofVerify (chal, pp, P) is an algorithm of TPA evidence verification. The chal, framework public parameters pp and auditing proof P are used as input. The TPA will confirm that evidence P is right**.**

Algorithm Execution Flow

Step 1: Start

Step 2: if (input = = Setup (k))

Then output = msk, pp.

Step 3: if (input = = Extract (pp, msk, ID))

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

Then output = skID.

Step 4: if (input = = SigGen (F, skID, ssk, name))

Then output = F*, Φ, τ.

Step 5: if (input = = Sanitization (F*, Φ))

Then output = F', Φ'.

Step 6: if (input= = ProofGen (F', Φ', chal))

Then output = P.

Step 7: if (input = = ProofVerify (chal, pp, P))

Then output = auditing proof P.

Step 8: End.

6. EXPERIMENTAL RESULTS

The authorized user of the system has access permissions such as adding patient details, downloading the patient data, signature verification and computation graph.

Fig: 2. Doctor Access Permissions

The owner can add the patient details such as patient name, contact number, email, address, disease description, and hospital name. Only the owner can view the data in an unencrypted manner.

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

Fig: 3. Patient details

The owner is allowed to view the graph.

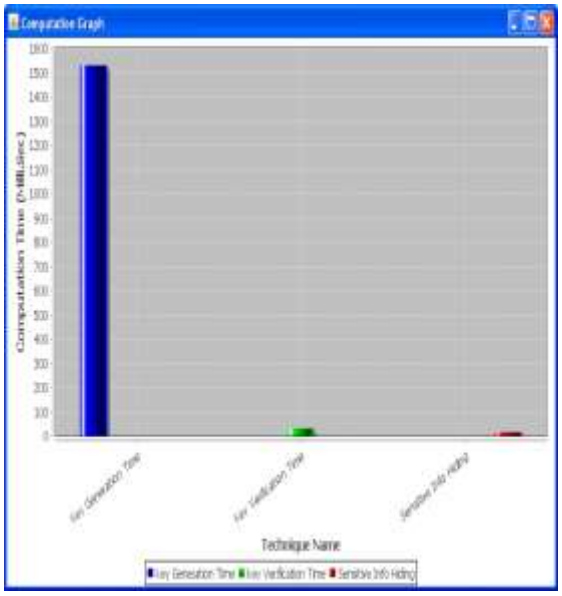

Fig: 4. Computation Graph

The unauthorized user has no access permissions except viewing the patient data in an encrypted manner. Here, disease description is the non-private information so there is no need of encrypting it.

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

Fig: 5. Encrypted data

The overhead calculation for the generation and verification of signatures is given below.

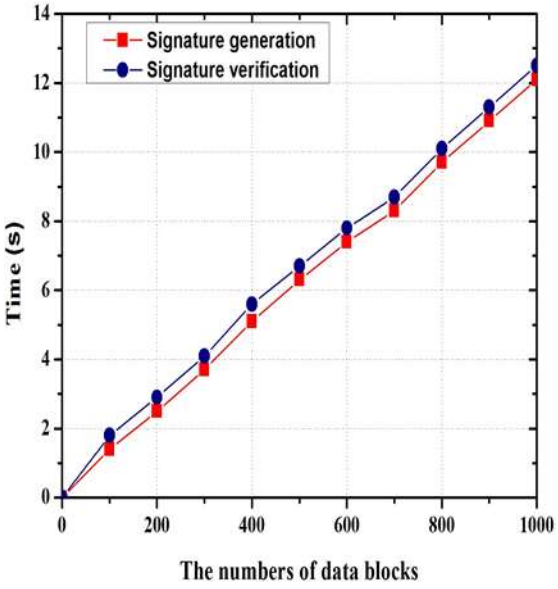

Fig: 6. Signature generation and Verification Graph

7. CONCLUSION AND FUTURE WORK

In this paper, we proposed identity based shared data integrity verification with hidden private information for reliable cloud storage, which encourages data sharing with hidden private information. This allows the data that is placed in the cloud to be shared and used by others based on the condition that the record's private information is guaranteed. The safety facts and exploratory investigation indicate that the conspiracy proposed to achieve desired safety and efficacy. For future work, data deduplication can be implemented which is used to remove duplicate files and also improves cloud storage capacity.

REFERENCES

[1] 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.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D.Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.
[3] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.
[4] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.
[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.
[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.
[9] 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.
[10] G. Ateniese, R. D. Pietro, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, pp. 1–10.
[11] C. Erway, C. Papamanthou, and R.Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, 2009, pp. 213–222.
[12] 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.
[13] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.
[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, June 2016.
[15] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.
[16] 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," Information Sciences, vol. 442-443, pp. 158 – 172, 2018.
[17] 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.
[18] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, no. C, pp. 130–139, Mar. 2016.
[19] 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," IEEE Transactions on Big Data, 2017. [Online]. Available:DOI:10.1109/TBDATA.2017.2701347
[20] 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.
[21] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in Proceedings of the 2015 IEEETrustcom/BigDataSE/ISPA- Volume 01, ser. TRUSTCOM '15, 2015, pp. 434–442.
[22] H. Wang, "Identity-based distributed provable data possession in multi cloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015.

ISSN- 2394-5125 VOL 08, ISSUE 04, 2021

[23] H. Wang, D. He, and S. Tang, "Identity-based proxy oriented data uploading and remote data integrity checking in the public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.

[24] Y. Yu, M. H. Au, 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," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017.

[25] H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," IEEE Transactions on Services Computing, 2016. [Online]. Available:DOI:10.1109/TSC.2016.263326.

[26] 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," IEEE Transactions on Dependable and Secure Computing, 2018. [Online]. Available:DOI:10.1109/TDSC.2018.2829880.

[27] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacy preserving authenticators for cloud storage," Future Generation Computer Systems, vol. 76, no. Supplement C, pp. 136 – 145, 2017.

[28] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable signatures," in Proceedings of the 10th European Conference on Research in Computer Security.