SECURING DATA USING TRUSTED THIRD PARTY AUDITOR FOR SECURE CLOUD STORAGE

Sujeethra. R
B.E/CSE
Francis Xavier Engineering College
Email:sujeethraramakrishnan@gmail.com

Narmadha.G
B.E/CSE
Francis Xavier Engineering College
Email:ganeshnarmu@gmail.com

Mrs N.Raja Priya M.E
(AP/CSE)
Francis Xavier Engineering College
Email:nrp.priya10@gmail.com

ABSTRACT

Cloud Storage Service, users can remotely store their data to the cloud and realize the data sharing with others. A cloud storage system consisting of a collection of storage server provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern data secrecy. In system the task of allowing a third party auditor (TPA) on behalf of the cloud client to verify the integrity of the dynamic data stored in the cloud. While prior works on ensuring remote data integrity often lac the support of either public audit ability or dynamic data operations, this system achieves both. First identify the difficulties and potential security problems has been direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our design .System, to achieve efficient data dynamics, to improve the existing proof of storage models by manipulating block tag authentication.

Introduction

The data storage and sharing services provided by the cloud, people can easily work together as a group by sharing data with each other.Share the latest version of the shared data with the rest of the group. Due to the existence of hardware/software failures and human errors In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. Most of the previous works focus on auditing the integrity of personal data.

Existing System

In Existing the document or file which is being stored by client in the cloud computing means that was stored entirely due to this someone can able to hack that so, hacker can able to see all the information's of the uploaded file.The system model involves five kinds of different entities: the cloud, the user, the sanitizer, the Private Key Generator (PKG) and the Third Party Auditor The cloud provides enormous data storage space to the user. Through the cloud storage service, users can upload their data to the cloud and share their data with others. The user is a member of an organization, which has a large number of files to be stored in the cloud. The sanitizer is in charge of sanitizing the data blocks corresponding to the sensitive information (personal sensitive information and the organization's sensitive information) in the file, transforming these data blocks' signatures into valid ones

for the sanitized file, and uploading the sanitized file and its corresponding signatures to the cloud.The PKG is trusted by other entities.When the TPA need to check the integrity of the sanitized file stored in the cloud ,it sends an auditing challenge to the cloud. And then, the cloud responds to the TPA with an auditing proof of data possession. , The TPA checks the integrity of the sanitized file by checking whether this auditing proof is correct or not.To efficiently support data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage, our scheme is designed to achieve the following goals: 1) The correctness:

Proposed System

Here we are providing better security in owner's upload side as well as on the download side.

For better security client splitting that single file into nine different blocks and providing a unique identification number for each block.

Using Honor Algorithm we are converting a block tag into secret value using ASCII value.

In order to achieve data sharing with sensitive information hiding, we consider making use of the idea in the sanitizable signature [30] to sanitize the sensitive information of the file by introducing an authorized sanitizer. However, a lot of chameleon hashes exhibit the key exposure problem. To avoid this security problem, the signature used in [30] requires strongly unforgeable chameleon hashes, which will inevitable incur huge computation overhead [31]. Secondly, the signature used in [30] does not support blockless verifiability. It means that the verifier has to download the entire data from the cloud to verify the integrity of data, which will incur huge communication overhead and excessive verification time in big data storage scenario. Thirdly, the signature used in [30] is based on the PKI, which suffers from the complicated certificate management.

Client

An entity, which has large data files to be stored in the cloud computing and relies on the cloud computing for data maintenance and computation, During login for a client here an OTP was generated and that was sent to the registered mail id using that OTP only a client can login.

Trusted Party Auditor (TPA)

This using a public auditing in proposed an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud computing storage services on behalf of the clients upon request.For better security using an AES algorithm 128 bit security.sd

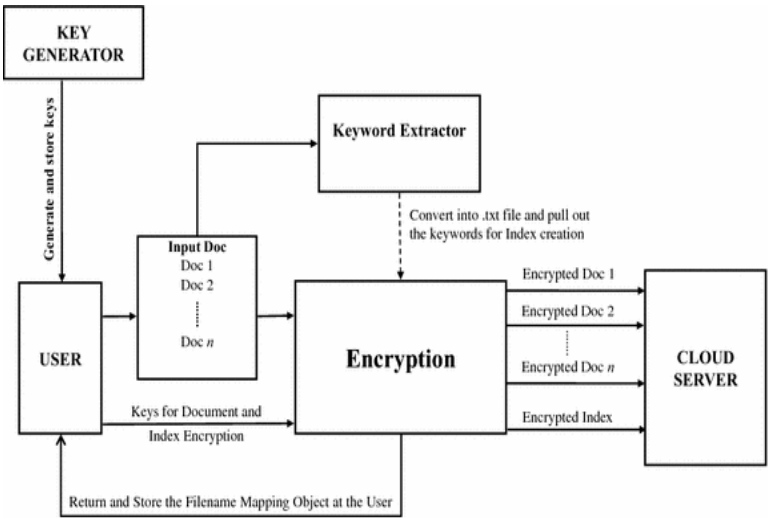

Fig :Systematic Design

Experimental Analysis

The user can also encrypt data before outsource it into the cloud server with encryption techniques .A significant research area for system protection, data access control has been evolving in the past thirty years and various techniques have been developed to effectively implement fine-grained access control, which allows flexibility in specifying differential access rights of individual users. Traditional access control architecture usually assume the servers storing the data are in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor responsible for defining and enforcing access control policies.

In order to verify the integrity of the data stored in the cloud, many remote data integrity auditing schemes have been proposed. To reduce the computation burden on the

user side, a Third Party Auditor (TPA) is introduced to periodically verify the integrity of the cloud data on behalf of user. Ateniese et al. [2] firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud. In their proposed .scheme, homomorphic authenticators and random sampling strategies are used to achieve blockless verification and reduce I/O costs. Juels and Kaliski [3] defined a model named as Proof of Retrievability (PoR) and proposed a practical scheme. In this scheme, the data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and BLS signature, Shacham and Waters [4] proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme.

In order to protect the data privacy, Wang et al. [5] proposed a privacy-preserving remote data integrity auditing scheme with the employment of a random masking technique. Solomon et al. [6] utilized a different random masking technique to further construct a remote data integrity auditing scheme supporting data privacy protection. This scheme achieves better efficiency compared with the scheme in [5]. To reduce the computation burden of signature generation on the user side, Guan et al. [7] designed a remote data integrity auditing scheme based on the indistinguishability obfuscation technique. Shen et al. [8] introduced a Third Party Medium (TPM) to design a light-weight remote data integrity auditing scheme. In this scheme, the TPM helps user generate signatures on the condition that data privacy can be protected. In order to support data dynamics, Ateniese et al. [10] firstly proposed a partially dynamic PDP scheme. Erway et al. [11] used a skip list to construct a fully data dynamic auditing scheme. Wang et al. [12] proposed another remote data integrity auditing scheme supporting full data dynamics by utilizing Merkle Hash Tree. To reduce the damage of users' key exposure, Yu et al. [13–15] proposed key-exposure resilient remote data integrity auditing schemes based on key update technique [16].

Experimental Results

In this subsection, we evaluate the performance of the proposed scheme by several experiments. We run these experiments on a Linux machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use C programming language with the free Pairing-Based Cryptography (PBC) Library [35] and the GNU Multiple Precision Arithmetic (GMP) [36]. In our experiments, we set the base field size to be 512 bits, the size of an element in to be |p| =160 bits, the size of data file to be 20MB composed by 1,000,000 blocks, and the length of user identify to be 160 bits.

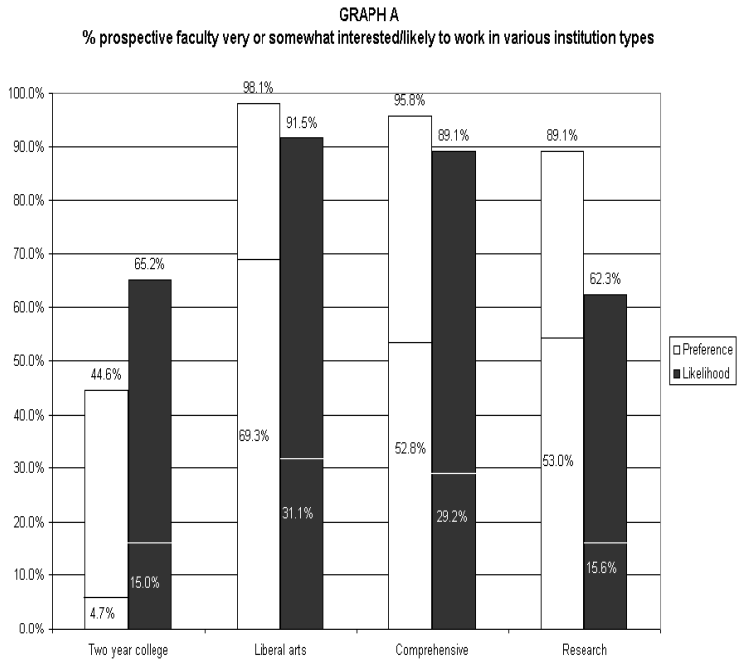

Fig: Experimental Result

Conclusion

A privacy-preserving public trusted third party auditing system for data storage security in Cloud Computing. We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. The TPA may concurrently handle multiple audit sessions from different

users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple trusted third party auditing tasks in a batch manner.

References

- Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011. Cloud Computing, pp. 295-302, 2012.
- M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
- K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
- D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
- B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013. .
- G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.
- Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.
- B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems,"
- Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.
- C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
- B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.229 5611.
- 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.
- G. Ateniese, R. D. Pietro, L. V. Mancini, 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.
- C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, 2009, pp. 213–222.
- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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
- 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.
- 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 IEEE Trustcom/BigDataSE/ISPA - Volume 01, ser. TRUSTCOM '15, 2015, pp. 434–442.
- H. Wang, "Identity-based distributed provable data possession in multicloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015.
- H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.
- 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.
- 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.2016.2633260
- 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
- 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.
- J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, Aug 2016.
- 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.
- 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, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 159–177.
- 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.
- 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 Transactions on Dependable and Secure Computing, 2017. [Online].Available: DOI:10.1109/TDSC.2017.2662216
- H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.
- J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2402– 2415, 2017.
- B. Lynn, "The pairing-based cryptographic library," https://crypto.stanford.edu/pbc/, 2015.
- "The gnu multiple precision arithmetic library (gmp)," http://gmplib.org/.