ISSN:0975-9646

Management of User Revocation with Public Auditing for Shared Data in the Cloud.

ANJU T G,
PG Scholar, Dept. Of CSE
Vidya Academy of Science and Technology
Thrissur, India

SIVADASAN E T,
Asst.Professor,Dept. Of CSE
Vidya Academy of Science and Technology
Thrissur, India

Abstract: Cloud computing is the biggest innovation ,which uses advanced computational power and it improves data sharing and data storing capabilities. Main difficulty with cloud computing was data integrity, data privacy and data access by unauthorised users. TTA (Trusted Third Party) is used to store and share data in cloud computing. With data storage and sharing services in the cloud, users can easily modify and share data as a group. In this project to verify the integrity of the shared data, members in the group needs to compute signatures on all shared data blocks. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. User revocation is one of the biggest security issue in groups. During user revocation shared data block signed by revoked user needs to download and re-sign by existing user .The existing systems downloads the entire file and verifies them to resign.This task is very difficult due to the large size of shared data blocks on cloud. Since a novel public auditing mechanism introduced for maintaining integrity of shared data with efficient user revocation in the cloud.This mechanism is based on proxy re-signatures concept, which allows the cloud to re-sign blocks on behalf of existing users during user revocation, so that downloading of shared data blocks is not required. It also monitor batch to verify multiple auditing tasks simultaneously .

Index Terms— Cloud computing, Data integrity, Public auditing, User revocatio, Batch auditing.

1.INTRODUCTION:

CLOUD computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. With data storage and sharing services provided by the cloud, people can
easily work together as a group by sharing data with each other. More specically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable envi- ronment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/ software failures and human errors. In this public auditing for shared data with efficient user revocation in the cloud , propose a novel public auditing mechanism for the integrity of shared data with effcient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures once a user in the group is revoked, the cloud is able to re-sign the blocks, which were signed by the revoked user, with a re-signing key. As a result, the efciency of user revocation can be signicantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, who is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties which traditional proxy re-signatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Moreover, which indicates it is not only able to effciently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing.

2. LITERATURE REVIEW

[A] Techniques used in Public Auditing on Cloud

There are different techniques which used for auditing mechanisms. This section introduce some the techniques like MAC, HLA etc. which are used for different purposes such as data authentication, data integrity in auditing schemes on cloud.

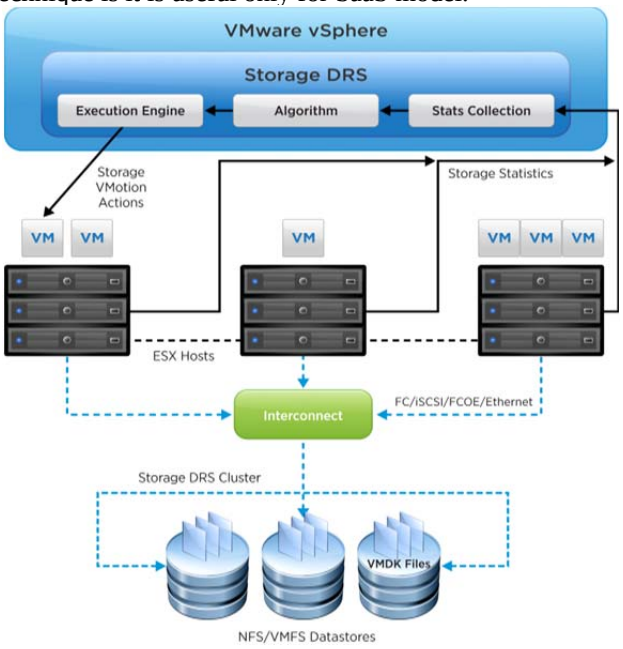
MAC Based Solution : MAC based technique is used for the data authentication. In this user upload data blocks with MAC and the Cloud provider provides Secret key to TPA. Here TPA will retrieve data blocks randomly and MAC uses SK to check the correctness of data. Online burden to users due to limited use (i.e. Bounded usage) and stateful verification is the main limitation of this method.

Using EAP : Using EAP they proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) . As compare to SSL authentication protocol APCC is more lightweight and efficient. It also used Challenge handshake authentication protocol (CHAP) for authentication. By using EAP, first the client request for any service to cloud service provider , then SPA send a CHAP request or a challenge to the client. When client recieves the challenge, client will sends CHAP response which is calculated by using the hash function to SPA. And finally SPA checks the challenge value with its own calculated value . If they are matched then SPA sends CHAP success message to the client.

Using Automatic Protocol Blocker : Automatic Protocol Blocker technique for error correction which checks data storage correctness . When an unauthorized user access user data, a small application runs which monitors user

inputs, It matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. Automatic protocol technique have five algorithms as keygen , SinGen, GenProof, VerifyProof ,Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and Pblock.

Using Virtual Machine : when user request CSP for service CSP authenticate the client and provide a virtual machine by means of Software as a service. Virtual Machine (VM) uses RSA algorithm for cryptography, where client encrypt and decrypt the file. SHA-512 algorithm is also used for making the message digest and check the integrity of data. This also helps in avoiding unauthorised access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.



HLA Based Solution : HLA performs auditing without retrieving data block. HLA is nothing but unforgettable verification meta data that authenticate. It checks integrity of data block by authenticating it in linear combination of the individual blocks. This technique allows efficient data auditing and consuming only constant bandwidth, but its time consuming as it uses linear combination for authentication.

[B].Different Public auditing mechanisms on Cloud.

Provable Data Possession at Untrusted Stores:It introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof[13]. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. We present two provably-secure PDP schemes that are more ecient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by crypto-graphic computation.

Privacy Preserving Public Auditing: Cloud computing is the future of the next generation architecture of IT solutions. Cloud provides computing resources on subscription basis over the internet. The Cloud data storage network includes a Third Party Auditor which has the power and capabilities that a client does not have[7]. It is a trusted entity that has the access to, other than cloud and check on the exposed risk involved in cloud storage data on behalf of the client. In this paper, the problem of data security and integrity has been presented. Also, a scheme to provide maximum data integrity. In this preserving scheme, can audit the data integrity without decrypting it. In the existing systems require round of interaction, User first has to create challenge and only then server can authenticate output with respect to challenge .The above delegation allow anyone to evaluate chosen encrypted data and non-interactively authenticate the output user needs to outsource all of data in one shot and stores some small secret state associated with the data to verify computation.Thus data can be easily predicted if decrypted by other than TPA .

This mechanism is based on 4 algorithms:

• Keygen: It is a key generation algorithm for setup the scheme.

• Singen: It is used by the user to generate verification metadata which may consist of digital signature.

• GenProof: It is used by CS to generate a proof of data storage correctness.

• Verifyproof: Used by TPA to audit the proofs

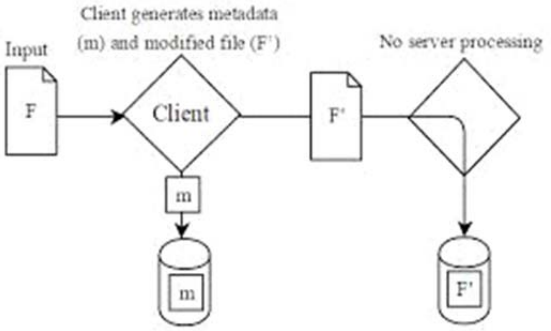
Provable Data Possession at Untrusted Stores :

Giuseppe Ateniese et all introduce a model which based on provable data possession (PDP). This is used for verifying that server is processing the original data without retrieving it. In this model probablistic proof of possession is generated by sampling random sets of blocks from the server.This helps to reduces I/O cost.

The main contributions of this technique are:

• Formally dene protocols for provable data possession (PDP) that provide probabilistic proof that a third party stores a file.

• Introduce the rst provably-secure and practical PDP schemes that guarantee data possession.



CONCLUSIONS:

The public auditing for shared data with efficient user revocation in the cloud , gives a new public auditing mechanism for shared data with effcient user revocation in the cloud. When a user in the group is revoked, It allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. The cloud can improve the efciency of user revocation by using the Proxy resignature scheme, and existing users in the group can save a signicant amount of computation and communication resources during user revocation.

BIBLIOGRAPHY

[1] M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography, Proc. Intl Conf. the Theory and Application of Cryptographic Techniques (EUROCRYPT98), pp. 127- 144, 1998

[2] M. Armbrust, A. Fox, R. Grifth, 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.

[3] 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 (CCS07), pp. 598-610, 2007

[4] H. Shacham and B. Waters, Compact Proofs of Retrievability, Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT08), pp. 90-107, 2008

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, Ensuring Data Storage Security in Cloud Computing, Proc. 17th ACM/IEEE Intl Workshop Quality of Service (IWQoS09), pp. 1-9, 2009

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling Public Veriability and Data Dynamic for Storage Security in Cloud Computing, Proc. 14th European Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009

[7] C. Wang, Q. Wang, K. Ren, and W. Lou," Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", Proc. IEEE INFOCOM, pp. 525-533, 2010.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verication of Outsourced Storages in Clouds", Proc. ACM Symp. Applied Computing (SAC11), pp. 1550-1557, 2011.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou," Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Jan. 2012.

[10] Y. Zhu, G.-J. Ahn, H. Hu, S.S. Yau, H.G. An, and C.-J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Trans. Services Comput-ing, vol. 6, no. 2, pp. 227-238, Apr.- June 2013

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, LT "Codes-Based Secure and Reliable Cloud Storage Service", Proc. IEEE INFOCOM, pp. 693-701, 2012.

[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Veriability and Constant Communication Cost in Cloud", Proc. ACM Intl Workshop Security in Cloud Computing (ASIACCS-SCC13), pp. 19- 26, 2013

[13] H. Wang," Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, Oct.- Dec. 2013

[14] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", Proc. IEEE CLOUD, pp. 295-302, 2012.

[15] S.R. Tate, R. Vishwanathan, and L. Everhart, "Multi-User Dynamic Proofs of Data Possession Using Trusted Hardware", Proc. Third ACM Conf. Data and Application Security and Privacy (CODASPY13), pp. 353-364, 2013

[16] B. Wang, B. Li, and H. Li, Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud, Proc. 10th Intl Conf. "Applied Cryptography and Network Security "(ACNS12), pp. 507-525, June 2012

[17] B. Wang, S.S.M. Chow, M. Li, and H. Li, Storing Shared Data on the Cloud via Security-Mediator, Proc. IEEE 33rd Intl Conf." Distributed Computing Systems "(ICDCS13), pp. 124-133, July 2013.

[18] M. van Dijk, A. Juels, A. Oprea, R.L. Rivest, E. Stefanov, and N. Triandopoulos, Hourglass Schemes: "How to Prove That Cloud Files are Encrypted", Proc. ACM Conf. Computer and Comm. Secu- rity (CCS12), pp. 265-280, 2012.