IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Survey on Ring Authentication in Multi-Cloud Environment

Harshitha K[1], Poornima B G[2]

PG Scholar, Dept. of CSE, Vidya Vardhaka College of Engineering, Mysuru[1]

Associate Professor, Dept. of CSE, Vidya Vardhaka College of Engineering, Mysuru[2]

Abstract: The follow of using remote servers massed on internet to store and manage data is known as cloud computing. Both the hardware and systems software in the data centre provides the application services on the internet. Integrity of data storage in cloud has become a major confront. Hence, facilitating public auditability for cloud is important with intension that users can route to a Third party Auditor (TPA) to check integrity. TPA executes audit for multiple users all together efficiently. This paper brings out a survey on different auditing mechanisms.

Keywords: Cloud Computing, Integrity, Public Auditing, Third Party Auditor (TPA).

1. INTRODUCTION

Due to the advantages such as on-command self-service, Omni-present network access, location-autonomous resource pooling, usage-based pricing and devolution of risk, the cloud computing has been visualized as the next generation information techno-logy (IT) architecture.
The main notion of the cloud computing is dynamic scalability which holds application data in a flexible manner. The user stores the data in cloud without any concern about precision and integrity of the data. The data stored by the users can be shared by various users across the cloud.

As, there are a number of providers of the cloud and the number of clients are increasing, security is fretful. There is a pressure between the user data protection and computation in the cloud. Thus, enabling public auditing mechanism for cloud is significant to the user and hence the users can way out to the Third-Party-Auditor (TPA). The TPA should guarantee that it does not bring a new susceptible towards user data privacy while introducing the security features.

Another important consideration is that how to preserve the user's identity from TPA, because the identities of signers on the shared data may indicate the particular user in the group. Therefore, several mechanisms have been defined to bear the public auditing mechanism. During this mechanism the share data is kept private from the TPA.
The data that is stored by the user in the cloud will be checked at the regular intervals to maintain the integrity. The cloud service provider will provide counter measures to improve security.
To prevent the malicious and frequent access the user has to input the equivalent verification code. To evaluate the loss, the user cannot have a conviction on the TPA. Thus, the integrity checking task is passed on to the proxy. Then, the proxy will achieve the integrity checking of the data according to their necessitate.
This survey paper focuses on different mechanisms to provide privacy of both user and the data in the cloud.

2. RELATED WORK

Micheal Armbust et al.[1] proposed an overview of cloud computing. Cloud computing is an overcome of adding as an utility, has the potential to transform a large part of IT industry, making software more attractive in the form of a service and shaping the way IT hardware is designed and purchase. Developers need not be worried about over-provisioning for a service. The statistical multiplexing are used to achieve elasticity and virtualization of each resources of how they are implemented and shared. Finally, it is declared that the cloud computing will grow and moreover application softwares will be both scale up and scale down according to the need of the users and the infrastructure software will be running on VMs also, the hardware systems should be designed at the scale of the container.

K.Ren et al.[2] proposed a privacy preserving public auditing system using the homo-morphic linear authenticator and random masking. Due to this procedure the TPA does not learn about the user detail while checking the integrity of the data. They also introduced creating one time passwords with key generation to overcome the security issues. The data is divided into blocks and each block is encrypted with secret key. An overt active scheme is proposed which supports the dynamic activities of the system.
Bo Chen et al.[3] describes Remote Data Checking (RDC) method by which clients can create the data which is farm out at un-trusted servers. With this tool clients can check the data integrity periodically. RDC also focuses on reducing the cost of the prevention phase. Remote data Checking for Network Coding (RDC-NC) provides cover against corruption attacks and replay attacks and also maintains a constant client storage. Thus, RDC-NC scheme can be used to make sure data remains undamaged when faced with data corruption, replay and pollution attacks.
B. Wany et al.[4] propose an auditing mechanism for the integrity of the shared data used by the people who work

together by sharing data as a group. The proxy re-signatures are used which allow the cloud to re-sign blocks on behalf of existing users during repudiation. Thus, the efficiency of the user repudiation and also computation saving is improved.

Boyang Wang et al.[5] introduced an public auditing mechanism for integrity of shared data with efficient user revocation in mind. The cloud re-sign the blocks in behalf of the user by utilizing proxy re-signatures. Also, the public verifier is able to audit the integrity of shared data without retrieving the entire data from the cloud. Therefore, the users in the group can save a significant amount of computation and communication resources during user revocation.

Francese Sebe et al.[6] proposes an overview of the data possession in networked information system. The Remote Data Checking protocol permits checking that the remote server can access an file without the knowledge of the verifier. By using the Diffie-Hellman based approach the efficient computation is achieved. The data is split into pieces and for each fragment a value is computed and stored. The verifier then sends the challenge to the prover. Next, the prover computes the value and resends to the verifier. Finally, the verifier checks the integrity. To perform the above method an ordering between the sets of files is defined.

Zhuo Hao et al [7] proposes a MR-PDP protocol which provides clients to check multiple replicas stored at the cloud storage. This protocol contains the public verifiability which increases the protocol's flexibility in the third-party-auditor. Homo-orphic authentication tags based on BLS signature are used in the protocol. The protocol is proved that is secured critical of malicious servers and also it preserves the file privacy against the third-party-auditor. It is proved that protocol is highly efficient through the performance analysis.

3. CONCLUSION

The data integrity can be achieved by various public auditing mechanism. The most important part is that the Third-Party-Auditor should be able to check the integrity without downloading the entire of the data. All the public auditing mechanism stores the data in the form of blocks and each block is encrypted and each block is encrypted with the signature of the user. From the survey, it can be concluded that a mechanism with higher efficiency can be used safe lock the data.

REFERENCES

[1] 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.

[2] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[3] 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.

[4] B. Wang, S.S. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator,” Proc. IEEE 33rd Int’l Conf. Distributed Computing Systems (ICDCS’13), pp. 124-133, 2013.

[5] B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

[6] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J. Quisquater, “Efficient Remote Data Integrity checking in Critical Information Infrastructures”, IEEE Transactions on Knowledge and Data Engineering, 20(8), pp. 1-6, 2008.

[7] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J. Quisquater, “Efficient Remote Data Integrity checking in Critical Information Infrastructures”, IEEE Transactions on Knowledge and Data Engineering, 20(8), pp. 1-6, 2008.

DOI 10.17148/IJARCCE.2016.5482