

A Survey on Improving Cloud Security using Data Integrity

Naveen N.¹ Prof. Dr. R. Vijayakumar²

¹M.Tech Student ²Professor

^{1,2}School of Computer Sciences, MG University, Kottayam, India

Abstract— Cloud computing is an internet oriented memory space that data can be fetched through internet. In recent years cloud computing is getting more attention because of the innovation in hardware and software resources, the ability to manage them remotely with benefits like high computing power, competitiveness, cost efficiency, scalability, flexibility, accessibility and availability, just adding more to the interest. There are many pros to cloud computing but on the other hand the security and integrity of data that gets stored in untrustworthy server is a determinant factor. Remote data integrity is playing a vital role in modern cloud storage and existing protocols are not secure enough under the quantum computer attacks. That is, attackers can hack the information sometimes from cloud even if data integrity protocols were installed. In this paper, a survey on cloud security by data integrity and auditing technique is done.

Key words: Cloud Security, Data Integrity, Cloud Auditing

I. INTRODUCTION

Cloud computing is an Internet based technology where the users can attain quality of services from data and software that resides solely in the remote servers. Basically it provides many advantages for the users to create and store data in the remote servers thereby utilizing fewer resources in client side. Cloud computing allows customers and businesses to use applications without installation and access their personal files at any computer with internet access anywhere in the world. As it is publicly available the security mechanisms are of highly concern. Nowadays, many institutions or organizations are moving to cloud storage. The data can be easy store or upload the data in the cloud platform. Furthermore, we can retrieve the required file or data effortlessly. This process will be done only with the help of internet access. The main purpose of the cloud is to keep our huge data very secure. Virtual machines allow simultaneous operation for more than an operating system furthermore, it provides the same processing to the numerous interconnected computers, as well it has an ability to reside the entire computing environments into one physical environment.

According to the large-scale organization, this was one of the first public networks, which allowed computers to access data from anywhere in the world.

In cloud storage, remote data integrity checking is considered as a crucial technique about data owners who upload enormous data to cloud server provider. A majority of the existing remote data integrity checking protocols rely on the expensive public key infrastructure. In addition, the verification of certificates needs heavy computation and communication cost. The idea is to secure against cloud service provider attacks, and leaks no any blocks of the stored file to the third party auditor during verification stage, namely the data privacy against the curiosity third party auditor attacks. Data integrity is nothing but verifying the data once we successfully upload the data into the cloud. No need to

download the whole content of data to verify, without downloading also we can check the integrity.

II. LITERATURE SURVEY

Literature survey is mainly focused and explained with the update of problems and data security measures.

Yves Deswarte and Jacques[2] introduced the first RDPC to analyze Data Integrity and represents how data is to be stored. Also he introduced two new ideas to store the data secure on cloud. Conventional challenge response being the first one and Diffie-Helman being the second one. Both of them can be considered as major achievements for that project. But the necessity to access the files for every solution, is the downside of this technique.

Giuseppe Ateniese, Randal Burn[3] introduced two updated ideas to overcome problems on the previous idea. That is provable data possession. Verification of unknown server is being done here. Guarantee and security are to be processed on both two techniques respectively. The RSA algorithm was the idea behind two of these factor. A constant amount of metadata is being also maintained on client side. There is no need to access file blocks here that has been stored on cloud database. But it doesn't support the dynamic operation.

Wang et al[4] introduces Merkle hash tree and this is for acquire the operations that are executed dynamically. The basic problem on cloud is said to be Security. Proposal of this Merkle hash tree is because of this security reasons. Because it supports the remote data integrity and authentication process to the server. These feature makes it highly effective and secured one.

A privacy preserving protocol also has been developed as a continuation for this. Basically auditor doesn't knows anything about data while it check together in cloud. For this homomorphism and masking are to be used. Both are combined together for the effective result. But there is a con here as existing PPAP will not supports the auditing on public side. Finally Wang finds an auditing protocol having batch verification for multi user.

R. PatilRashmi[5] introduced updated data possession protocol that can resist the attack of the active adversary. It is purely based upon the homomorphic hash function. Continues checking of data integrity is the major process here so that the integrity of data is to be calculated continues. Merkle hash tree is being used on this protocol also so that data location can be calculated. Dynamic operations like insert, modify, delete and update supports at this condition. Also the base aspect is that, auditing also works together to find the correctness and accuracy. But it have no confidentiality.

III. CONCLUSIONS

In this Survey paper describes many methods of cloud security. RDPC was the first idea to find data integrity on a data base. Many algorithms like RSA are also implemented

later with encryption mechanism. The Merkle hash tree makes a vital change in cloud security and data integrity, while also increasing the factors regarding security. New protocols like privacy preserving protocols are also used for auditing the data base in later techniques, improving upon the existing ideas. With those aspects data possession protocol is the update done for all the protocols and it get replaced as well. It makes resistance against the attackers, hackers, and also supports all the dynamic operations related to cloud.

REFERENCES

- [1] S. Suganya and P.M Durai Raj Vincent "Improving Cloud Security by Enhancing Remote Data Integrity Checking Algorithm", Proc.IEEE International Conference on Networks & Advances in Computational Technologies (NetACT), 2017.
- [2] Y. Deswarte, J.J. Quisquater, and A. Saïdane, "Remote integrity checking." Proc. IEEE in Integrity and internal control in information systems VI, pp. 1-11, 2004.
- [3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Proc.IEEE In Proceedings of the 14th ACM conference on Computer and communications security, pp. 598-609.Acm, 2007.
- [4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li. "Enabling public auditability and data dynamics for storage security in cloud computing," Proc. IEEE transactions on parallel and distributed systems, Vol. 22 No. 5, pp. 847-859, May 2011.
- [5] Rashmi, R. Patil, and S. M. Sangve. "Public auditing system: Improved remote data possession checking protocol for secure cloud storage," Proc.IEEE International Conference on Applied and Theoretical Computing and Communication Technology, pp. 75-80, IEEE, Oct 2015.