A Survey on Security Issues in Cloud Environment

Mrs.R.Ahila[1], Dr.S.Sivakumari[2]
[1]*Assistant Professor, Dept of Information Technology*
[2]*Professor & Head, Dept. of Computer Science and Engineering, Faculty of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women*

Abstract - Cloud computing is an emerging technology with promising future is becoming more and more popular nowadays. It is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. In Cloud simplicity the data and application software moved to cloud data centers.The Cloud service provider should ensure integrity, availability, privacy and confidentiality. The service provider is not providing the reliable data services to customers and to stored customer data. This study related to cloud data storage security issues such as data theft, data breaches and unavailability of cloud data.This paper deals with the possible solutions to respective issues in cloud.

Keywords - Cloud computing, auditing protocols, cloud service, cloud data security.

I. INTRODUCTION

Nowadays the cloud computing [1] is becoming more popular in IT organizations and developers. The cloud computing technology provides the virtualized computer power, storage and services on demand for customers. The important factors in cloud computing is confidentiality, integrity, availability preserving the data hence the data is stored in the distributed database. The integrity defined as restrict the unauthorized person to access the data. The availability defined as the data being available for access at any time. The internet plays a fundamental role in the cloud computing it represents either the medium or the platform through which is used to increase the cloud services. The Cloud Computing Services [2] are offered as the Infrastructure as s service (IaaS), Platform as a service (PaaS), and Service as a service (SaaS). The IaaS services used to develop the scalable web sites or for background processing. The PaaS services increases level of the abstraction and act as the middleware platform which is used to creating abstract environment where the applications are deployed and executed. The SaaS services providing the application on demand services. The main goal of the cloud computing technology is make best utilization of the distributed resources and achieve the higher throughput and remove large scale computation problem. The cloud storage [3] is the one of the major services in the cloud computing which provides great benefits to the user. The one of the important security problem in the cloud is how efficiently check the data integrity in the cloud environment. The several auditing protocol [4] proposed to overcome this issue such as dynamic authentication protocol, Batch auditing protocol etc.

In recent days the key exposure problem arising in cloud storage auditing which is reduces the security of the cloud environment. To solve this issue in this paper the cloud storage auditing [5] with verifiable outsourcing of key updates proposed. In this scheme the key updates are not performed by the client but by an third authorized party (TPA). The TPA holds an encrypted secret key of the client for cloud storage auditing and key updates under encryption state in each time period. The client download the encrypted secret key from the authorized party and decrypts occur only the client would like to upload new files to cloud. Additionally the client also verifies the validity of the encrypted secret key. The TPA also checks the integrity of the clients files stored in the cloud. The blinding technique with homo morphic property used to form the encryption algorithm to encrypt the secret keys which is held by the TPA.

II. CLOUD SECURITY ISSUES

(i) The strong key exposure resilient auditing scheme proposed for overcome the key exposure problem. The novel and efficient key update technique used in this scheme. The third party Auditor generates the updated message from user secret key at each time period then its send to the client. The client update his signing secret key only depends upon user private key and update message from the TPA. This technique makes the malicious cloud not able to obtain the signing secret keys in unexposed time periods. So the new technique able to do key updates for unlimited time periods.

(ii) The cloud data auditing mechanism with identity based integrity checking (ID-CDIC) proposed to further improve the strong key exposure resilient auditing scheme. The ID-CDIC technique construction from the RSA signature which is used to support the variable sized file blocks and public auditing. The ID-CDIC technique secure under the well-known RSA assumption.

(iii) The efficient public auditing scheme proposed to enhances a public auditing scheme with both identity privacy and identity traceability for group members. The proposed scheme construct mainly for shared cloud data, in which identifies the group members are anonymous to the TPA and the group manager can identify the dishonest member while the dispute occur. To protect the identity privacy of group members, a group manager is generating the authenticators of data blocks for the group members. At the same the identity traceability achieved through the group manager in where the latest record modification of each data block in the list. If the group member maliciously modifies the shared cloud data the group

manager easily fined him/her depends upon the list. Additionally the blind signature technique achieve the data privacy while authenticator generation.

(iv) In fourth work a novel integrity auditing scheme proposed for improving the computation performance of efficient public auditing scheme. The novel integrity auditing scheme supports multiple writer for cloud based data sharing services. The proposed scheme design on polynomial authentication tags which is used to empower the cloud to aggregate authentication tags from the multiple writers into one when sending the integrity proof information to the verifier. The verifier only need the constant size of the integrity proof information and the constant number of the computational operation and does not consider the size of the audited file and how many writers associated with the data blocks. The proposed scheme also allows the secure delegation of the user revocation operation in the cloud environment and which can defeat impersonation attacks from illegitimate users. The proposed scheme also allows aggregation of integrity auditing operations for multiple tasks through the batch integrity auditing technique.

III. METHODOLOGY

Cloud Service Provider (CSP) and Third Party Auditor (TPA) are shown in Figure1 Clients - The Clients are those who have data to be stored, and access it with help of Cloud Service Provider (CSP). They are such as tablet, desktop computers, laptops, mobile phones, etc.

Cloud Service Provider (CSP):- Cloud Service Providers (CSPs) are those who have major resources and proficiency in construction, managing distributed cloud storage servers and provide applications, infrastructure, hardware, enabling technology to Clients as a service via internet.

Third Party Auditor (TPA):- Third Party Auditor (TPA) who has expertise and capabilities that Client may not have and verifies the Integrity of data stored in cloud on behalf of Clients. Based on the audit result, TPA could release an audit report to the Client.

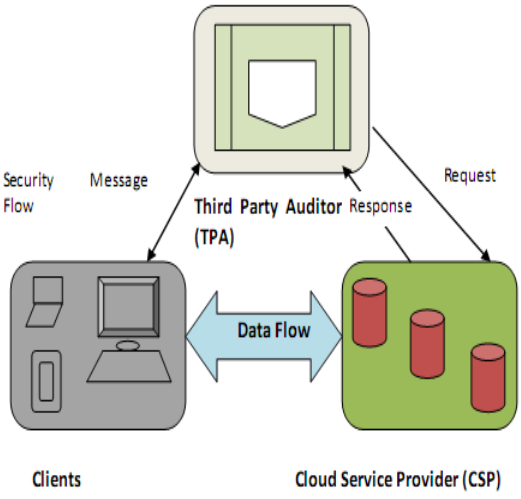

Fig.1: Cloud Auditing System

In cloud computing technique, the Clients store their data files in cloud and access them with the help of Cloud Service Provider (CSP) whenever and wherever they need. The cloud consists of a set of cloud servers, which are consecutively in a concurrent, cooperated and distributed approach. Data redundancy is utilized with method of erasure-correcting code to additionally accept responsibilities or server crash as user‘s data and encrypting the data can prevents the data leakage. Additionally, the Clients frequently verify the Integrity of data without having a local copy of data file. Unauthorized access and misuse of customers' confidential data are serious concerns regarding data outsourcing. Hence, it is of significant importance to be aware of data administrators (CSPs) and extension of data access right.

IV. CONCLUSION

In this paper discussed about various solutions to on how to ensure that data stored in cloud is not maligned or corrupted by the service providers or other attacks agents using various types of methods in order to test the service provider for quality of data provided and ensuring data is correct.

V. REFERENCES

[1]. Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2017), “Dynamic remote data auditing for securing big data storage in cloud computing” ,Information Sciences, 380, 101-116.

[2]. Garg, N., & Bawa, S. (2016), “Comparative analysis of cloud data integrity auditing protocols” ,Journal of Network and Computer Applications, 66, 17-32.

[3]. Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. (2012), “Efficient audit service outsourcing for data integrity in clouds”, Journal of Systems and Software, 85(5), 1083-1095.

[4]. Yu, J., Ren, K., Wang, C., & Varadharajan, V. (2015), “Enabling cloud storage auditing with key-exposure resistance”, IEEE Transactions on Information forensics and security, 10(6), 1167-1179.

[5]. Yu, J., Ren, K., & Wang, C. (2016), “Enabling cloud storage auditing with verifiable outsourcing of key updates”, IEEE Transactions on Information Forensics and Security, 11(6), 1362-1375.

[6]. Anirudha Pratap Singh and Syam Kumar Pasupuleti, 2016. “Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing”, Procedia Computer Science, Vol. 93, pp.751-759.

[7]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, 2011. “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.

[8]. Kan Yang, and Xiaohua Jia, 2013. “An efficient and secure dynamic auditing protocol for data storage in cloud computing”, IEEE transactions on parallel and distributed systems, Vol. 24, No. 9, pp. 1717-1726.

[9]. Jianhong Zhang, Qiaocui Dong, 2016. “Efficient ID-based public auditing for the outsourced data in cloud storage”, Information Sciences, Vol. 343, pp. 1-14.

[10]. Lu Rao, Hua Zhang, and Tengfei Tu, 2017. “Dynamic Outsourced Auditing Services for Cloud Storage Based on Batch-Leaves-Authenticated Merkle Hash Tree”, IEEE Transactions, pp. 1-14.

[11]. Rajat Saxena and Somnath Dey, 2016. "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing", Procedia Computer Science, Vol. *89*, pp. 142-151.
[12]. Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability." *Journal of Systems and Software* 113 (2016): 130-139.
[13]. Jiawei Yuan and Shucheng Yu, 2015. "Public integrity auditing for dynamic data sharing with multiuser modification", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 8, pp. 1717-1726.
[14]. Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, and Jian Shen. "Cloud data integrity checking with an identity-based auditing mechanism from RSA." *Future Generation Computer Systems* 62 (2016): 85-91.
[15]. Jia Yu, Kui Ren and Cong Wang, 2016. "Enabling cloud storage auditing with verifiable outsourcing of key updates". *I*EEE Transactions on Information Forensics and Security, Vol. 11, No. 6, pp. 1362-1375.
[16]. Xu, J. (2011). Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage. IACR Cryptology EPrint Archive, 2011, 304.
[17]. Ganjali, A., & Lie, D. (2012, October). Auditing cloud management using information flow tracking. In Proceedings of the seventh ACM workshop on Scalable trusted computing (pp. 79-84). ACM.
[18]. Xie, R., & Gamble, R. (2013, January). An architecture for cross-cloud auditing. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (p. 4). ACM.
[19]. Shao-hui, W., Su-qin, C., & Zhi-wei, W. (2012). Public auditing for ensuring cloud data storage security with zero knowledge Privacy. pp-1-12.
[20]. XU, C. X., HE, X. H., & Daniel, A. (2012). Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing.