Survey on Secured Proxy Based Distributed Data Storage in Public Cloud Database

Nasrin Banu A, Information Technology, IFET College Of Engineering, Villupuram, India

Sindhuja K, Information Technology, IFET College Of Engineering, Villupuram, India

Mrs Suganthi V, Associate Professor, IFET College Of Engineering, Villupuram, India

***Abstract*— Cloud computing is the collection of networked computers sharing the resources on-demand. The increasing use of cloud computing over the globe has brought into focus a need to design a secure cloud storage system. The feasibility and usefulness has made cloud computing a popular growing field. But placing confidential data outside the place of an organization and in hands of cloud providers should come with guarantee that our data should be secure and available at any point of time. We tend to propose associate design for higher security and confidentiality of an information hold on within the cloud databases. When the information are stored and accessed through the cloud server, security is the main concern, where there is a possibility complicity of data contents. The complicity occurs because the cloud servers are not fully trustable. To overcome cyber trials in cloud, we have proposed an architecture, in which data is encrypted and then stored. Some of the cloud users may prefer a privacy enhanced data management while they are sharing their personal data over the public cloud. The focal point of this paper is security concerned privacy enhancement of data in the cloud environment.**

***Index Terms*— Cloud computing, Security, Cyber trials, Privacy enhancement, Data management**

I . INTRODUCTION

Today user may spend lot of time with a computer to collect lot of data over network and store it where it as portable for the user. During the roaming time user may need the data from their PC (Personal Computer) it is very difficult to take it as a portable one with large datasets. So they may problem occurred while their roaming time. For this reason storing an enough data in network can solve this problem .Could storage is used to avoid this problem .Cloud storage refer to storing a large amount of data which in the form of pay-per-use scheme which is referred to cloud computing .It is used to off-site storage scheme maintained by a third party i.e. cloud provider [1]. Some of the major issues of cloud computing are Data security, Costing model, Charging model, Service Level Agreement, migration and Cloud interoperability Issues [2]. We are focusing on the security issues [3] in cloud in this paper. A recent report by Kaspersky Security solution, a Russian based cyber security company places countries like U.S, China and India prone to cyberattacks. So security is the major issue in computing world. In some cases user have worry about the security and privacy problem from the cloud provider. In some cases cloud provider provide a security to the frontend resource only and failed to provide a security to the backend resources, so the attackers may hack the data easily from the backend resources.

Hence malicious user could compromise the data integrity and confidentiality. Where leakage details of data might be in the user cloud resources and the cloud provider are the responsible for this issue [4].The possible types of security attacks present in the cloud computing environment are SQL injection attacks, Cross site scripting attacks, Man in the middle attack, Denial of service attack, and Sniffer attack. Thus user must provide a security from the cloud provider between the attackers and the forgoing cloud resources by encrypting their data. Encryption is a process of encoding the data in some format i.e. embedding the text in the format of cipher text to protect data managed by untrusted server.

ISSN: 2278 – 7798

The privacy preservation of the cloud user is the most important role of the service providers where the most confidential information of users is stored in the cloud. The users do not want to share their information with others where the data are shared publicly among the cloud. Some of the issues, leads cloud service providers to attain privacy is insufficient user control, Information disclosure, unauthorized second storage, uncontrolled data proliferation, and Dynamic provision.

The manner in which information could be stored in the cloud could be either centralized or distributed. The advantage with centralized storage is that it is easy to handle. However, distributed storage is a challenge to the data owner and impractical to implement. Most of the real world systems incorporate a combination of centralized and distributed storage systems. Besides, relying on a third party cloud storage provider could lead to security problems. To assure data confidentiality, data owner stores an encrypted data in the cloud. It is good to use Attribute Based Encryption instead of ordinary encryption techniques. Key Policy – Attribute Based Encryption (KP-ABE), an encryption scheme was suggested to make the cloud storage more secure [5]. Cipher text Policy – Attribute Based Encryption (CP-ABE) is designed to overcome the limitations of KP-ABE [6]. An encryption scheme namely Hierarchical Attribute Based Encryption (HABE) scheme is formed by combining Hierarchical Identity Based Encryption (HIBE) and CP-ABE.

II. LITERATURE SURVEY

In this Survey relative mechanisms and the methods which are employed earlier to attain a security and privacy are discussed. C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, [7] focuses on achieving secured and dependable storage in the cloud environment where the data are outsourced publicly in distributed manner. The effective way of achieving secured cloud storage is analyzed. To overcome this problem a flexible distributed storage integrity auditing mechanism is proposed. The framework of this work consists of three components, namely user, Cloud Server (CS), Third Party Auditor (TPA). Cloud provider is responsible for providing significant storage space to the cloud user for storing their data. TPA is responsible for providing trusted access. This work evaluates dynamic data verification in order to provide secure dependable data storage. The method proposed in this work [7] is highly efficient and resilient to Byzantine attacks. However the redundant copies present in multiple servers may lead to the memory unavailability and high cost.

Data Integrity cannot be performed accurately due to the dynamic nature of behavior at multiple copies stored in multiple servers. The efficiency of the data sensitive application can be improved by data redundancy. However, data redundancy in the cloud may lead to the cost effective problems as described in [7] where the clouds are the pay per use model. N. cao, [8] proposed a secure cloud storage service to overcome the reliability problem with optimal performance .Maintaining privacy, reliability and availability for data security is a function of the correct application and security mechanisms at various level in the cloud infrastructure. Among these mechanisms [10][9][11] are a broad range of components that implement verification and access control. Validation of users and even of communicating system is performed by various cryptographic techniques. Authentication of users take several forms [12][13], but all are based on a combination of authentication factors: something an individual knows (such as a password),something they possess (such as a security token).Single feature authentication is based on only one authentication requires additional factors, for instance, two factor authentication is based on two authentication factors (such as a pin and a fingerprint).

Preliminary work in this field was limited to cryptographic file systems and secure storage solutions. There is a previous study regarding network file systems [14], in which study is made regarding how to keep data securely onto untrusted servers. An another architecture [15] i.e. Depot is a two level architecture which guarantees security of data stored in cloud, even after malicious attacks i.e. it can tolerate the faults, attacks and can preserve confidentiality. But [14] and [15] don't support the computations on the encrypted data, so this architecture are not much helpful in implementing our goal. Many service providers guarantee

confidentiality [16] by dividing the data of a single user and then storing it into different clouds so as the cloud provider will be unable to get the data in whole. The data is restored by accumulating these cloud providers. But the hindrance is that if all the distributed parts are gained by some of the cloud providers the confidentiality is at state.

Luca Ferretti , Michele Colanjannni and small Marchetti proposes " Distributed, Synchronic and Temporary access to Encoded Cloud Databases" in which they propose a unique design that integrates cloud information services with knowledge confidentiality and therefore the risk of corporal punishment synchronic operations on encrypted knowledge. The planned design has the additional advantage of eliminating intermediate proxies that limit the physical property, accessibility and scalability properties that are intrinsic in cloud- based solutions. Yu et al. bestowed a scalable and fine-grained knowledge access management theme in cloud computing supported the KP-ABE technique. The knowledge owner uses a random key to write a file, wherever the random secrets additional encrypted with a collection of attributes victimization KP-ABE. Also said that to reach user revocation, the manager gives tasks of knowledge file recoding and user secret key update to cloud servers.

A re-encryption scheme was advised to enhance the data security in untrusted clouds [17]. A cloud environment consists of many cloud servers. The owner needs to encrypt the data before storing it into the cloud. To avoid the revoked users accessing the data file with their decrypt keys, the contents must be re-encrypted and the new keys are rendered to the authorized users. Four cloud servers namely CSS1, CSS2,CSS3 and CSS4 have been considered. The data owner needs to re-encrypt all the old cipher-text using the new encryption keys. For this purpose, re-encryption in all cloud servers.The revoked users gain the old cipher-text which is decrypted key by their old decryption keys if the server is not updated due to network failures. Muhammad Rizwan Asghar et.al [18] discusses the problems of enforcing security policies in cloud environment. With the high growth of data in cloud they were problem arises due to untrusted person access of the data.

To ensure the security is immature, they didn't ensure for the safe data in cloud environments. Security problem is a great issue; here we enforce the security for the owner's data. Providing high security they may high expensive for the users. For the above mentioned problem Muhammed Rizwan Asghar et.al proposed an ESPOON policy which is Encrypted Security Policies for outsourced environments. This policy is used to address the above problem and give better confidentiality to the users. It provides a better security by separating the security policy and the enforcement mechanism. Chen et al. in 2014 proposed that bundle the data with access policy and sending this bundle to authorized use untrusted applications this proposed Architecture called Data Safe. This Data Safe Mechanism allows only to the authorized user to set out the policy to the data so that it can accessible only from the trusted party [19].

III. CONCLUSION

Cloud computing is one of the important for the cloud user to access the data through network at anywhere. So they were worried about the security problem of their personal data. In this survey we present threats and solution for security and privacy for the data owner upload the cloud user. Various types of possible ways to overcome these issues are analyzed. Our proposed work to provide privacy, it is necessary to give high security for the data before uploading into the cloud. This can be achieved by encrypting the data into the cloud database. Here the data owner who upload the data or files into the cloud through secure database and the owner sharing a data user with the secret key. The data owner can decide the access permission independently with the help of the private key generator. Only one data can be access for a request, instead of all the data's.

REFERENCES

[1] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Distributed, concurrent, and independent access to encrypted cloud databases." (2014):1-1.

[2] Kuyoro S. O , Ibikunle F. and Awodele O**.,** "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), VOL.3, No.5, 2011.

[3] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication.

[4] Arora, Indu, and AnuGupta. "Cloud Databases: A Paradigm Shift

in Databases. "*International J. of Computer Science Issues* 9.4(2012): 77-83.

[5] V.Goyal, O. Pandey, A. Sahai, B.Waters, "Attribute-based encryption for fine grained access control of encrypted data,"CCS., 89–98,2006.

[6] J. Bethencourt, A. Sahai, B. Waters, "Cipher text- policy attribute based encryption, "IEEE S&P., 321–334,2007.

[7] Cong Wang, Qian Wang, KuiRen, NingCao and WenjingLou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Volume: 5, Issue:2, April-June2012, ISSN:1939-1374.

[8] NingCao, ShuchengYu, ZhenyuYang, WenjingLouandY. ThomasHou, "LT Codes- based Secure and Reliable Cloud Storage Service", Proceedings of IEEE Info com, 2012, ISSN: 0743-166X.

[9] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved Proxy Re encryption Schemes with Applications to Secure Distributed Storage. ACMT Trans. Inf. Syst. Secure., 9:1-30, February2006.

[10] Saman Zarandioon, Danfeng Yao, and Vinod Ganapathy. K2C: Cryptographic Cloud Storage with Lazy Revocation and Anonymous Access. In proceeding of secure comm, 2011.

[11] H. Xiong, X. Zhang, W. Zhu, and D. Yao. Cloud seal: End- to-End Content Protection in Cloud-based Storage and Delivery Services. In proceeding of secure comm,2011.

[12] L. Zhou, V. Varadharajan, and M. Hitchens. Enforcing role-based access control for secure data storage in the cloud. The c omputer Journal, 2011.

[13] F. Hansen and V. Oleschuk, "SRBAC: A Spatial role-based access control model for mobile systems," in proc of 8thNordiac Workshop on Secure IT Systems (NORDSEC), October 2003.

[14] J. Li, M. Krohn, D. Mazieres, and D. Shasha, " Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Operating Systems Design and implementation, Oct. 2004.

[15] P.Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish,"DEPOT: Cloud Storage With Minimal Trust" ACM Trans. Computer Systems, vol.29, no. 4, article 12, 2011.

[16]v.Ganapathy, D.Thomas, T.Fedrer,H.Gracia Molina and R.Mothwani,"Distributed Data For Secure DataBase Services," Proc.Fourth ACM Int'l Workshop Privacy and Anonmyity in the Information Soc., Mar. 2011.

[17] Qin Liu, Chiu C. Tan, Jie Wu, and GuojunWang, "ReliableReencryption in Unreliable Cloud," Proc.Of Globecom, 2011.

[18] Muhammed RizwanAsghar, Mihaela Ion, Bruno Crispo,"ESPOON Enforcing Encrypted Security policies in outsourced Environments" 2011 Sixth International Conference on Availability, Reliablity and Security.

[19] Mao Tan, Youzhi Li, "Design and Implementation of General Distributed Heterogeneous Data Exchange System" 978-1-61284-486-2/11 2011 IEEE.

AUTHORS BIOGRAPHY

Ms NASRIN BANU A, currently pursuing B.Tech, Information Technology at IFET College of Engineering, Villupuram, India. Her area of interest includes Oops Concept, Cryptography and Cloud Computing.

Ms SINDHUJA K, currently pursuing B.Tech, Information Technology at IFET College of Engineering, Villupuram, India. Her area of interest includes Core Java, Asp.Net, and Mobile Computing.

Mrs SUGANTHI V, received her B.E, in CSE from Jayaram college of Engineering and Technology, Bharathidasan University and her M.Tech in IT from Sathyabama University. She has got one year of Industry Experience. She is currently working as an Associate Professor in the department of Information Technology, IFET College of Engineering, and Villupuram, India. She has published three International Journal. Her area of interests includes Computer Networks, Programming paradigms and Network Security.