# Survey on Cloud Storage Data Security

**Aishwarya Prajapati[1], Prof. Sumit Nema[2]**
[1]Dept of CSE
[2]Assistant Professor, Dept of CSE
[1, 2] Global Nature Care Sangathan Group of Institution, Jabalpur, Madhya Pradesh, India.

***Abstract-*** *Cloud Computing is next generation computing technology with the dynamic capabilities of adding new resources and services as per user demand and requirement. Cloud computing is fast growing technology which facilitates more and more users and organizations shifting towards opting their services to cloud. Data security is considered as the constant issue leading towards a hitch in the adoption of cloud computing. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing. The advent of the proposed model has sufficient functionalities and capabilities which ensures the data security and integrity. The proposed framework focuses on the encryption and decryption approach facilitating the cloud user with data security assurance. The proposed solution only talks about the increased security but does not talk about the performance. In this paper, a survey of different security issues and threats are also presented. A data security framework also provides the transparency to both the cloud service provider and the cloud user thereby reducing data security threats in cloud environment.*

***Keywords***- Cloud Security, Integrity, Availability, Data Security Issues.

## I. INTRODUCTION

Cloud computing is an open standard model which can enable ubiquitous computing and provide network access to a shared group of configurable computing resources. It provides distributed computing environment consisting hardware, software and services [1]. Apart from this, it provides storage space and support execution of various services and data processing [2]. Cloud security handles the weakness and susceptibility of cloud computing [3]. Cloud security can be categorized as: Cloud Data Security and Storage Security. Data security ensures the privacy and confidentiality of shared data while the storage security ensures the correctness of the uploaded data stored in untrustworthy cloud servers. But cloud computing has many challenges regarding both data and storage security [4].

### *A. Data Security*

While sharing the data in cloud space, the cloud service provider (CSP) can completely acquire access to all user data. So, data sharing bring challenges in terms of security in cloud computing. The main privacy and security requirements of data sharing in cloud are: Data Confidentiality and User revocation.

### *B. Storage Security*

*Cloud* Data Owners (CDOs) upload their local data into the cloud. If some CSPs are dishonest, they may conceal the data loss or error from the users for their own benefit. Moreover there are chances that they might delete rarely accessed user data for saving storage space. Therefore, CDOs need to be ensured about the correctness of data stored in the cloud [5] [6]. Another challenge is verifying the integrity of stored data [7].

## II. SURVEY ON CLOUD SECURITY

Some of the existing survey works on security issues of cloud computing is discussed below. Naresh vurukonda et. al. [8] has made a study which identified the issues of cloud data storage, identity management and access control. Possible solutions were suggested for some of the issues.

Ayesha Malik et al [9] have defined a methodology for cloud providers that protect users' data and important information. In their study, they have explained different characteristics of the cloud computing, different service models etc.

Yunchuan Sun et al [10] have reviewed different security solutions for data storage security and privacy protection in cloud computing. They have presented a comparative research analysis of the existing techniques regarding data security. Mazhar Ali et al [11] have discussed various security issues of cloud computing. Their survey consists of latest security solutions along with complete discussion on security issues. They also provided a brief discussion on security issues and solutions related to mobile cloud computing. Sultan Aldossary et al [12] have discussed the issues of cloud data storage and solutions. The survey included issues of virtualization, data integrity, data

availability, data confidentiality. Apart from these data security issues, they have listed out various threats on cloud computing.

## III. SURVEY OF DATA AND STORAGE SECURITY

*A. Classification of Security in Cloud computing* As shown in Figure 1, the data Security issue in Cloud Computing able to be classified.

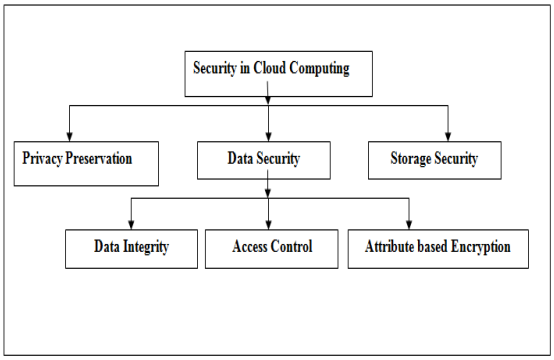


Fig.1.1: Security Classification in Cloud.

Furthermore data security is classified into three different categories.

- Privacy Preservation defines that Privacy of personal and important information in cloud is crucial as the cloud servers are not trusted. Confidentiality and authorization are main requirements of privacy preservation in cloud.
- Storage Security defines that Cloud storage Security is the task of providing integrity to the shared data stored at dishonest cloud servers.
- Data Security defines that the data or information security is the process of protecting the data from unauthorized users, preventing alterations and restricting the access of sensitive information.

### *B. Existing works on Privacy preservation*

Haralambos Mouratidis et al [13] have presented a security framework for selecting a cloud provider based on relevant security requirements. It consists of a modelling language and a tool using the Open Models Initiative (OMI) Platform. The language applies the principles of security and privacy.

L. Malina et al [14] have proposed a security model for cloud based on group signatures. It provides authentication and anonymity for user privacy. It also ensures confidentiality and integrity of transmitted data. Ulrich Greveler et al [15] have designed a cloud database architecture that prevents unauthorized access of uploaded data from the internal and external administrators. It uses XACML structure for describing the access control policy. The contents of the database are encrypted using an Encryption Proxy.

### *C. Existing works on Storage Security*

Kan Yang et al [6] have designed a privacy preserving auditing protocol for cloud systems. The protocol supports dynamic operations on data and batch auditing for multi-cloud environment. It uses bilinear pairing to generate an encrypted proof. The verification of the proof correctness is then executed by the data auditor. In this protocol, the computational overhead of the auditor is moved to the cloud server. However it fails to provide data confidentiality and user authorization.

Qian Wang et al [7] have a provided a verification scheme for storage security by integrating data integrity and dynamic data operations. In this scheme, an auditor verifies the integrity of storage data. The dynamic data operations include block insertion and deletion using Merkle Hash Tree (MHT) technique. They have applied the technique of bilinear aggregate signature for maintaining multiple auditing tasks. But it does not provide confidentiality and authorization.

Yan Zhu et al [8] have designed a Provable Data Possession (PDP) scheme for ensuring the integrity of cloud data storage. In PDP, multiple cloud service providers (CSPs) cooperatively maintain the client's data. The two main components of PDP are hierarchy using hash index and homomorphic verifiable response. It provides defence against leakage of data and forgery of tag attacks. But it does not provide confidentiality and authorization.

Lifei Wei et al [16] have proposed SecCloud which provides both secure storage and computation auditing features. By using verifier signature and batch verification techniques, it achieves privacy cheating discouragement. But it does not provide confidentiality and authorization.

### *D. Existing works on Data Security*

The three important characteristics of data security are listed below.

- Data Integrity: It is commonly assured by validations using cryptographic tools such as message digests, hashing and digital signature etc.
- Access Control (AC): An access control system includes components and methods to specify access control policies for legitimate users.

- Attribute based Encryption (ABE): The uploaded data is encrypted using ABE that defines access policy on attributes related to the data. Hence only authorized users with matching attributes can decrypt and access the data.

Younis A. Younis et al [1] have proposed a novel Access Control model for Cloud Computing (AC3) to satisfy the requirements of access control. It consists of three hierarchical levels of security based on the level of trust. In this model, users are classified according to their roles and assigned to corresponding security domains. But this work does not provide confidentiality and integrity.

Jin Li et al [2] have designed a fine-grained access control system based on ABE. AC policies are defined based on the data attributes. The accountability of user is implemented by applying the traitor tracing method. Furthermore user revocation and user grant operations are implemented by applying a broadcast encryption technique. But it results in huge communication overhead.

Yan Zhu et al [4] have presented encryption scheme for temporal access control (TACE). In this algorithm, the access policy contains temporal attributes of users based on which the access rights are defined. TACE enforces temporal constraints. But this work does not provide confidentiality and integrity.

Guoyuan Lin et al [17] have provided a trust based AC technique for cloud computing. It defines trust connections among users and cloud platform. It combines role-based access control (RBAC) with trust model. The trust model is formed by combining identity trust and behavior trust. But this work does not provide confidentiality and integrity.

Varsha D. Mali et al [24] have designed a trust based cloud storage system in which trust model is integrated with RBAC technique. But this work does not provide integrity and authentication.

Saravana Kumar et al [3] have proposed a new encryption technique based on ABE. It uses digital signature and asymmetric encryption algorithms with hash functions. But since the encryption technique is based on simple hash functions, it can be compromised.

Shulan Wang et al [18] have proposed a file hierarchy based ABE scheme for cloud computing. In this scheme, hierarchical files are encrypted using an integrated access structure. The ciphertext portions of attributes are shared by the files. But it does not provide data integrity. Moreover, it depends on single TA which may be subjected to failure.

Shulan Wang et al [19] have proposed an improved two-party key distribution protocol. In this protocol, any user's secret key cannot be compromised by either the key authority or CSP. Moreover, they have included weights for each attributes to enhance the expression of attribute from binary to arbitrary level. Because of this, the storage cost and encryption cost are reduced. But the access policy is not hidden and the single TA may be subjected to failure.

Tran Viet Xuan Phuong et al [20] have proposed CP-ABE scheme. In this scheme, AND-gate with wildcards is used to define the access policy. The access policy is protected using hidden ciphertext policy. However, the key escrow problem is not resolved.

Entao Luo et al [21] have proposed a hierarchical multi-authority and CB-ABE based friend discovery scheme. It uses character attribute subsets to avoid single point failure and performance overhead. But this work does not provide data integrity.

## III. CONCLUSION

In this survey work, the data security and storage security in cloud computing have been explained in detail. The different classifications in data and storage security are explained with the proposed techniques. From the survey it can be concluded that both data and storage security should be provided with less storage and computational overhead. In data security, authentication, authorization confidentiality and integrity should be ensured.

## REFERENCE

[1] Younis A. Younis, Kashif Kifayat and Madjid Merabti, "An access control model for cloud computing",Elsevier,journal of information security and applications,2014.

[2] Jin Li, Gansen Zhao, Xiaofeng Chen and Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.

[3] Saravana Kumar N, Rajya Lakshmi G.V and Balamurugan B, "Enhanced Attribute Based Encryption for Cloud Computing",Procedia Computer Science 46 ( 2015 ) 689 –696,2015.

[4] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang, "Towards Temporal Access Control in Cloud Computing", IEEE, 2012.

[5] Laicheng Cao, Wenwen He, Xian Guo, and Tao Feng, "A Scheme for Verification on Data Integrity in Mobile Multicloud Computing Environment", Mathematical

Problems in Engineering Volume 2016, Article ID 9267608, 6 pages,2016.

[6] Kan Yang, and Xiaohua Jia, "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, 2013.

[7] Qian Wang, Cong Wang,Kui Ren and Wenjing Lou, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing",IEEE,2009.

[8] Naresh vurukonda and B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing",Procedia Computer Science 92(2016) 128 – 135,2016.

[9] Ayesha Malik and Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences,VOL. 3, NO. 3, March 2012.

[10] Yunchuan Sun,Junsheng Zhang,Yongping Xiong, and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages,2014.

[11] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in Cloud Computing: Opportunities and Challenges", Elsevier,Information Sciences,2015.

[12] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016.

[13] Haralambos Mouratidis, Shareeful Islam, Christos Kalloniatis and Stefanos Gritzalis, "A framework to support selection of cloud providers based on security and privacy requirements", The Journal of Systems and Software, 2013.

[14] L. Malina, J. Hajny, P. Dzurenda and V. Zeman, "Privacy preserving security solution for cloud services", Journal of Applied Research and Technology, 2015.

[15] Ulrich Greveler, Benjamin Justus and Dennis Loehr, "A Privacy Preserving System for Cloud Computing", IEEE, 2011.

[16] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen and Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing", Information Sciences,2013.

[17] Guoyuan Lin,Yuyu Bie and Min Lei, "Trust Based Access Control Policy in Multi-domain of Cloud Computing" ,JOURNAL OF COMPUTERS, VOL. 8, NO. 5,May 2013.

[18] Shulan Wang, Junwei Zhou,Joseph K. Liu,Jianping Yu, Jianyong Chen, and Weixin Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, VOL. 11, Issue 6, June 2016.

[19] Shulan Wang, Kaitai Liang, Joseph K. Liu,Jianyong Chen, Jianping Yu, and Weixin Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 8, AUGUST 2016.

[20] Tran Viet Xuan Phuong, Guomin Yang and Willy Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 1, JANUARY 2016.

[21] Entao Luo, Qin Liu and Guojun Wang, "Hierarchical Multi- Authority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks", IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 9, SEPTEMBER 2016.