ISSN: 0975-766X
CODEN: IJPTFI
Available through Online
www.ijptonline.com
Review Article

A SURVEY ON VARIOUS SECURITY MEASURES USED IN CLOUD

P. Suganya
Assistant Professor, School of Info.Tech. and Engg. VIT University ,Vellore, India.
Email: pjkumar@vit.ac.in

Received on 14-02-2016 *Accepted on 12-03-2016*

Abstract

Securing data in the network has been an important task since the intrusion of various attacks that attempts to corrupt or hack data for malicious purpose. Various security mechanisms have been proposed in the literature to secure data from an unauthenticated user. The popular methods includes symmetric and asymmetric cryptographic mechanism which use keys distributed among the owner and authenticated users to access data genuinely. This approach works well in an environment where the numbers of users are less and the file being accessed is small in size. It consumes significant amount of overhead to generate keys and distribution of the same to the users. In addition when the size of the file is large it consumes more space to hold the encrypted form of the data. Cloud being a large scale distributed system that contains more number of storage nodes and users requires an optimized mechanism to offer security to the users of data with minimized communication overhead and reduction in storage spaces required to hold the encrypted form of the data. In this paper we analyse various approaches proposed to provide efficient data access to the users of the cloud. We also mention the possible extensions of the proposed approaches as future work

Keyword: Attribute based Encryption, Key distribution, Multi Authority

1. Introduction

Cloud emerged as a revolutionary computing paradigm offers various services to its user such as Software as Service (SaaS), Platform as a service (PaaS) and Hardware as Service [9] [10]. It offers almost infinite storage facility to store data in it. The access to data should be controlled so that only authenticated users can have an access to it. The conventional cryptography uses symmetric and asymmetric mechanism to convert data into cipher text. A key is generated for the encrypted data and it is given to the authenticated users.

The user can decrypt the data using the key. This approach involves in key generation, key distribution, user authentication and it should support storage space to hold the encrypted form of the data. It works well for network with a moderate number of users and systems. The number of racks and data nodes is very large in a cloud environment which stores large volume of data interconnected by communication network [8].

The conventional key generation and distribution mechanism consumes more communication overhead and it requires more storage space to hold the encrypted form of data. Cloud computing environment requires an efficient securing mechanism to control access to data with minimized communication cost and storage space. We analyse various approaches proposed in the literature for securing data access in cloud.

2. Various approaches for Security in Cloud

2.1 The work in [1] provides a comprehensive study on the issues and challenges in cloud. It considers the various basic properties of cloud such aselasticity, multi-tenancy and third party control. They have analysed the security requirement from the perspectives of confidentiality, availability, integrity, audit, trust and compliance. The work has proposed a security architecture that consists of access security, identity security, network security, infrastructure security, application security and hypervisor security.

2.2 The work in [2] proposed an effective data access control mechanism for cloud. It suggests that existing access control schemes can’t be implemented for cloud because they produce multiple encrypted copies of the same file or it requires a trusted server. It also identifies that CP-ABE based mechanism suffers from Decryption and revocation in multi authority cloud storage systems where users should hold multiple attributes. It proposed an effective Data access control for multi authority storage clouds and Extended Data access Control for multi authority storage

2.3 The work in [3] has studied the importance of security in cloud. It discussed about various cryptographic techniques proposed in the literature. It summarizes various techniques and its objectives. The techniques searchable encryption and attribute based encryption provides confidentiality for the data stored on the cloud. Attribute based encryption can also be used for access control in cloud.

Broadcast encryption is used for distribution of keys. XML encryption and group encryption are used for confidentiality .Group signature is used for access control.

2.4 The work in [4] discusses about medical image storage in cloud and provision of security. The emergence of cloud that offers storage as a service motivates users to store large volume of data in it. It acts as an exchange platform for medical practitioners to upload medical images obtained from Computer Tomography and Magnetic Resonance Imaging. However the stored data should be protected from various types of attackers in the network. The work [4] studies the impact of Denial of service attacks, Data Leakage attacks over the data stored in cloud.

2.5 The work in [5] discusses about providing security, additionally considering reliability and availability in managing resources in cloud.

2.6 The work in [6] proposed a multi keyword ranked search to search the content of the data stored in the cloud in an encrypted form. Data owners can store their data in cloud to offer service at an economically saving with flexibility. However the data should be encrypted to protect it from the public. Searching is usually performed using a single key that is looked into the content of data. Multi keyword searching approach proposed by [7] improves the search efficiency with reduced computational time and communication cost.

2.7 The work in [7] proposed a third party auditing scheme to audit the integrity of the data stored in the cloud to let the user free from worry. It extended its work to audit multiple users at the same time to improve the efficiency.

3. Conclusion

The importance of securing data in the cloud is studied in this paper. The drawbacks of conventional cryptographic schemes have been studied and various approaches used to provide security and access control to cloud data is reviewed**.**

4. References

1. HuagloryTianfield, “Security Issues In Cloud Computing”, IEEE International Conference on Systems, Man, and Cybernetics, 2012

2. Kan Yang et al, “DAC-MACS: Effective Data Access Control forMulti-authority Cloud Storage Systems”, IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, November 2013.

3. Peng Yong et al , “Secure cloud storage based on cryptographic techniques”,The Journal of ChinaUniversities of Posts andTelecommunications, Elsevier,October 2012, 19(Suppl. 2): 182–189

4. Shini.S.G et al, “Cloud Based Medical Image Exchange-SecurityChallenges”,Procedia Engineering, Elsevier 38(2012) 3454 – 3461.

5. Ravi Jhawar et al, “Supporting Security Requirements for ResourceManagement in Cloud Computing”,IEEE 15th International Conference on Computational Science and Engineering,2012

6. Ning Cao et al ,” Privacy-Preserving Multi-Keyword RankedSearch over Encrypted Cloud Data”, IEEE transactions on parallel and distributed systems, vol. 25, no. 1, January 2014

7. Cong Wangetal ,” Privacy-Preserving Public Auditingfor Secure Cloud Storage”, IEEE Transactions on computers, vol. 62, no. 2, February 2013.

8. Jenn-Wei Lin, C. H. Chen and J. Morris Chang, "QOS Aware Data Replication for Data Intensive Applications in Cloud Computing Systems", Early Articles, IEEE transaction on cloud computing, vol. 1, no. 1, pp. 101- 115, 2013, DOI:10. 1109/TCC. 2013. 1 Sep 2013.

Corresponding Author:
P. Suganya,
Email: *pjkumar@vit.ac.in*