International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 11: November 2015, pp 1-2. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey On Privacy-Preserving Authentication Protocols in Cloud Computing using VPS

Indusha K, Jayaraj R

***Abstract*—** This paper is to develop a Computational Private Information Retrieval protocols on cloud architecture using erasure code for secured data forwarding. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. In this paper we have discussed about the various authentication protocols. Related papers are taken survey and its advantage and disadvantages are discussed.

***Keywords*—** Cloud computing, authentication protocol, privacy preservation, shared authority, universal composability

I. INTRODUCTION

Cloud storage architecture will have a collection of storage servers with higher end configuration which will provides long-term storage services over the Internet and also for the cloud storage system. Here storing and retrieving the data in a third party's cloud system and public auditing scheme causes serious problems and conflict over data confidentiality during the data transactions. Whenever third party big data storage will involve with the cloud server this conflict will occur naturally. Even thou there are various methods are available to overcome this problem like cryptography, key encryption and etc. But general encryption schemes protect data confidentiality during the transaction, but along with this process the main drawback will, it limits the functionality of the storage system. These methods will cause failure. In order to constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. We proposes a secured threshold proxy re-encryption server and integrates it with a decentralized erasure code such that a secure distributed storage system is formulated for processing the data. In this method multiple users can interact with the storage system. The main technical contribution is that the proxy re-encryption scheme supports encoding operations along with a key over encrypted messages, as well as forwarding operations over encoded and encrypted messages. The content in the database will be in the decrypted format. So that even intruder cant able to access the big data even they access the database. The encrypted data will become unused even the data obtained by the intruder. This makes the system so stronger. This project deals with fully integrates encrypting, encoding, and forwarding. The storage and robustness are more flexible with the users. So that user will authorize the sender request to generate the key. Using the authorized one time key sender can access the encrypted file in decrypted format at once. The key will become invalid after one use. This is method is implemented for secured data forwarding. During data forwarding a proxy server will be created virtually to access the encrypted data from the sender side. The original data from the cloud server will be transmitted to the proxy virtually. After the transaction the proxy server will be deleted along with the data. So that data will be safe always in the cloud storage servers.

Indusha K, PG Scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India. (Email: indushafine16@gmail.com)

Jayaraj R, Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India. (Email: jayarajems@gmail.com)

II. VARIOUS SECURITY METHODS

S. No	TITLE	DESCRIPTION
1.	Cloud Computing: Networking and Communication Challenges[2]	This paper discuss about the incast problem, cost effective data center scalability, secured cloud access, unpredictable traffic patterns and variable demand, dynamic network resource allocation, workload and IP mobility, to name a few.
2.	On-Demand Security Architecture for Cloud Computing[3]	Cloud service providers (CSP's) exist between clients specifically data marts are more likely to take advantage of cloud computing platforms than operational, transactional database systems
3.	Proxy Provable Data Possession in Public Clouds[4]	To use ECC-based homomorphism authenticator to design PDP scheme, which does not compute expensive bilinear and consume small amount of calculation and Communications. This scheme is very suitable for mobile clouds.
4.	Privacy Preserving Data Sharing With anonymous ID Assignment[5]	This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access.
5.	KeyChallenges in Cloud Computing to Enable the Future Internet of Services[6]	Deploying future IaaS clouds and include efficiently managing such clouds to deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and technologies that let

		cloud providers collaborate and improving energy efficiency
6.	Trusted Cloud Computing with Secure Resources and Data Coloring[7]	This technique safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private cloud.
7.	Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage[8]	This is for ensuring the integrity of data in storage outsourcing. This introduces lower computation and communication overheads in comparison with non-cooperative approaches.
8.	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing[9]	An efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. It says that the auditing protocols are secure and efficient.
9.	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing[10]	This is to support efficient handling of multiple auditing task. Extensive security and performance analysis shows it is highly efficient and provably secure.
10.	Privacy Preserving Policy Based Content Sharing in Public Clouds[11]	A key advantage of the BGKM scheme is that adding users or revoking users or updating acps can be performed efficiently by updating only some public informations.

III. CONCLUSION

In this paper, we have discussed about various authentication techniques and protocols for data security in cloud computing. But some authentications protocols are too costly to implement in real time. The results of these protocols are analyzed. Compared to all the result Privacy Preserving Policy Based Content Sharing in Public Clouds gives the better result and is cost effective.

REFERENCES

[1] https://www.google.co.in/search?q=cloud+computing+Wikipedia&gws_rd=ssl

[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.

[3] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.

[4] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing,vol.6,no.4,pp.551559,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.

[5] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing,vol.6,no.4,pp.551559,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.

[6] R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, "KeyChallenges in Cloud Computing to Enable the Future Internet ofServices,"IEEEInternet Computing,vol.17,no. 4,pp. 18-25,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, July/Aug.2013.

[7] K. Hwang and D. Li, "Trusted Cloud Computing with SecureResources and Data Coloring," IEEE Internet Computing, vol. 14,no. 5, pp. 14-22, Sept./Oct. 2010.

[8] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,"IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12,pp. 2231-2244, Dec. 2012.

[9] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, Sept. 2013.

[10] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859-25, May 2011.

[11] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledgeand Data Eng., vol. 25, no. 11, pp. 2602-2614,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, Nov. 2013.