A SURVEY: CLOUD COMPUTING DATA SECURITY AND ACCESSING TECHNIQUE

Priya Sen[#1], Abhishek Sahu[*2]

[#]*CSE TIT College, RGPV University*
India
[2]psen8581@gmail.com

ABSTRACT: Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and un-trusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cloud Computing has been the most promising innovation in the computing world in past decade. Its usage is still hindered by the security concerns related with critical data. The encryption of remotely stored data has been the most widely used technique to bridge this security gap. The speculated vast usage of Cloud Computing solutions for data storage and with Big Data Analytics gaining strong foothold; the security on cloud is still at big risk. Fully Homomorphic Encryption is a good basis to enhance the security measures of un-trusted systems or applications that stores and manipulates sensitive data. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis is assumed to show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Keywords: Cloud computing, Health care domain, Security approach, data processing, Cloud Simulation, Symmetric Encryption.

INTRODUCTION

Cloud computing is a recent technological development in the computing field in which mainly focused on designing of services which can be provided to the users in same way as the basic utilities like food, water, gas, electricity and telephony. In this technology services are developed and hosted on the cloud (a network designed for storing data called datacenter) and then these services are offered to users always whenever they want to use.

The cloud hosted services are delivered to users in pay-per-use, multi-tenancy, scalability, self-operability, on-demand and cost effective manner. Cloud computing is become popular because of above mention services offered to users. All the services offered by servers to users are provided by cloud service provider (CSP) which is working same as the ISP (Internet service provider) in the internet computing. In the internet technology some innovative development in virtualization and distributed computing and accessing of high speed network with low cost attract focus of users toward this technology. This technology is designed with the new concept of services provisioning to users without purchasing of these services and stored on their local memory.

RELATED TERMS

Architecture

In the cloud computing architecture of service provisioning, basically three parties are involved for providing services to the users:-

1. User/Client
2. Third Party Auditor (TPA)
3. Cloud Server (CS)

LITERATURE REVIEW:

In this paper [1] author proposed:

1. A fully homomorphism encryption algorithm in the cloud computing data security.
2. This new security solution is fully fit for the processing and retrieval of the encrypted data and effectively leading to the broad applicable prospect the security of data transmission and the storage of the cloud computing .
3. It is convenient for users and the third party agency to search date to dispose. At present, fully homomorphic encryption scheme has high computation problem needs further study.

The author of the paper [2] proposed:

1. A technique in which they have described about the technique for cloud and data security and majorly they have highlighted the big data storage capacity in a cloud computing environment.
2. They have proposed a secure k-means data mining approach assuming the data to be distributed among different hosts preserving the privacy of the data.
3. The approach is able to maintain the correctness and validity of the existing k-means to generate the final results even in the distributed environment.

In this paper [3] Proposed:

1. A work TPA to perform audits for multiple users simultaneously and efficiently they performed batch auditing support where multiple file can be audit without knowledge of data to the tpa and cloud.

2. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

3. They have enables an external auditor to audit user's cloud data without learning the data content, multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner, MAC based setup has been performed and hashing algorithm is used to perform auditing while dealing with the data.

In this paper [4] they have proposed:

1. Secure User Data in Cloud Computing Using Encryption Algorithms proposed a scheme for cloud security they proposed different security algorithms to eliminate the concerns regarding data loss, segregation

and privacy while accessing web application on cloud.

2. Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud.

3. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM.

In this paper [5] proposed:

4.

1. A new short signature scheme from the bilinear pairings that unlike BLS uses general cryptographic hash functions such as SHA-1 or MD5.

2. It does not require special hash functions. Furthermore, the scheme requires less pairing operations than BLS scheme and so is more efficient than BLS scheme.

3. This signature scheme to construct a ring signature scheme and a new method for delegation. We give the exact security proofs for the new signature scheme and the ring signature scheme in the random oracle model.

Sr.	Author	Techniques	Advantage	Disadvantage
1	Xingliang Yuan, Xinyu Wang, Cong Wang	Fully homomorphic secure technique.	Privacy preserving approach.	Heavy computation for sub process.
2	Feng Xao	K-Mean data extraction approach.	Cluster based technique perform effective mining.	Less secure approach.
3	Deepti Mittal	MAC based setup in cloud environment.	MAC based approach perform device level security.	Limited to device.
4	K. Ren, C. Wang, and Q. Wang	DES algorithm for the data security.	Easy to implemented.	Less secure approach.
5	Quian Wang	BLS and SHA-1	Hashing technique and better auditing mechanism.	Less secure compare to other available techniques.

Table 1- Comparison between available approach.

EXISTING SYSTEM:

Existing work contains a framework which provides a proper security and data indexing, storage and accessing mechanism over the cloud.

Here are we have following main contribution done in existing work :

1. They have worked on health care domain in cloud computing.
2. They have worked on secure mechanism over the cloud data storage, reporting and other device level document relevant to medical field.
3. They have worked with proper storage mechanism thus a proper accessing can be done by end user.
4. They have worked with proper indexing mechanism for searching and secure accessing along with privacy preserving mechanism over medical data.
5. They have worked with Amazon cloud with homomorphic encryption in their mechanism for security.

PROBLEM DEFINITION

The existing system does not provide any sort of algorithm of approach in which a proper auditing can be provided.

- A proper auditing scheme is still require in homomorphic algorithm.
- No Digital signature or any embedded message is yet introduced to verify the correctness of data stored in cloud.
- User is not able to verify its data integrity.
- Data might be unsafe or might be not multiply maintained at cloud server if user applied or paid for it so.
- High capacity data storage issue.

CONCLUSION:

Here we have discussed about the literature and work which is already done in the field of cloud computing and its security concern, various models for security and data encryption and verification process been introduced in past, here we have study about the latest cloud security storage scheme which is homomorphic scheme. The scheme says about the run time encryption scheme while data modification and manipulation system without having the knowledge of data and information about the data length and its integrity, but still the system doesn't support verification system embedded with the homomorphic system, the homomorphic system still need to support with hashing technique, thus we are proposing here a hashing scheme embedded with homomorphic encryption data storage scheme which make our system more secure and efficient for the user.

REFERENCE:

1. Xingliang Yuan, Xinyu Wang, Cong Wang, "Enabling Secure and Fast Indexing for Privacy-assured Healthcare Monitoring via Compressive Sensing", IEEE 2016.

2. Feng Zhao , Chao Li , Chun Feng Liu, "A cloud computing security solution based on

fully homomorphic encryption, IEEE conference 2014.

3. Deepti Mittal, DamandeepKaur, Ashish Aggarwal The author of the paper entitled "Secure Data Mining in Cloud using Homomorphic Encryption", IEEE conference 2014.

4. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73,2012.

5. Qian Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011

6. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10,2008.
7. C. Wang, B. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

8. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), 2009.

9. K.D. Bowers, A. Juels, and A. Oprea, "Hail: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), pp. 187-198, 2009.

10. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from theWeil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), pp. 514-532.