A CLOUD STORAGE SYSTEM FOR SHARING DATA SECURELY WITH PRIVACY PRESERVATION AND FRAUD DETECTION

Manoj Shantaram Tore[1], S.K.Sonkar[2]

[1] PG Student, Computer Engineering, AVCOE Sangamner, Maharashtra, India
[2]Assistant Professor, Computer Engineering, AVCOE Sangamner, Maharashtra, India

Abstract

Cloud computing provides much-known services for storing user data over cloud server and it provides attention towards a broad set of technologies, rules and controls deployed to provide security for applications and data. As the more and more firm uses the cloud, security in cloud environment is becoming very important issue. It is much needed that companies should work with partners doing best practices of cloud security and which facilitate transparency for their solutions. Number of security solutions today depends on the authentication for security but it did not provide solution for the privacy problems while sharing data in the cloud environment. Data access request from the user itself may expose users' private data no matter his request approved or not. So this becomes very important in sharing data in the cloud environment. In this paper we proposed a system which provides attention towards the above mentioned problem. In proposed system we used the concept of data anonymity for sending data access request to data owner and also provide the data auditing facility to detect fraud in the integrity of users shared data.

Keywords: *Cloud computing, privacy preservation, data integrity, data sharing, authentication*

---***---

1. INTRODUCTION

Cloud computing offers mixing of data servers and web services in distributed computing fashion. Important firms like Amazon, Google, Microsoft, Yahoo, Salseforce and others provides cloud services to users. At the primary stage the architecture of cloud based services provided by amazon and after this different new models and variations has been proposed for cloud architecture. Many techniques available today for data storage over a cloud server so that client can be assured in terms of CIA triad, i.e confidentiality, integrity and availability of data on cloud servers. Confidentiality means that data is protected from the unauthorized entities. It can be ensure by different cryptographic techniques. Availability means the user can use his own data stored over cloud storage everywhere and anytime. Integrity means that actual data cannot be change by any unauthorized entities. Cloud computing technology can increase availability with the use of internet enabled access, but in this case user is restricted to timely and strong and healthy provision of resources. Availability is affected by the architecture of a cloud and capacity of cloud to store data of cloud provider. Fig-1 [1] shows the cloud computing environment which consists of three elements. First one is the cloud user who has the vast amount of data to be stored over cloud storage, second one is the cloud storage which is maintain by the cloud service provider which is able to facilitate storage services and has large storage space and computation resources and the last one is the Trusted Third Party (TPP) who has expertise and has the abilities that cloud user doesn't has. It is trusted to calculate cloud storage service reliability on behalf of user over user's request.

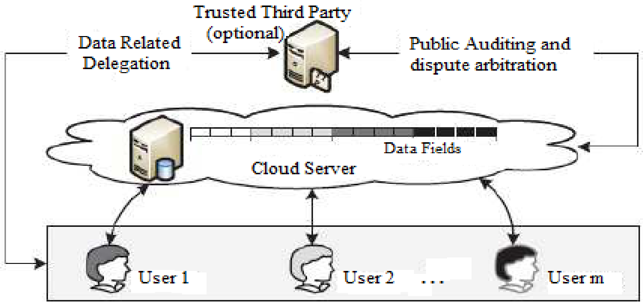
Trusted Third Party (optional)
Data Related Delegation
Public Auditing and dispute arbitration
Data Fields
Cloud Server
User 1
User 2
...
User m

Fig -1: Cloud Storage Environment

Users store their data remotely over cloud and take advantages of pull based high quality applications and services from a shared pool of configured computing resources using cloud storage, without any load of local data maintenance and storage. The other advantage of using a cloud services is that user can easily share their data with other cloud users for getting more and more profits. So data sharing in the cloud computing environment is an important functionality. Though data sharing is important in cloud computing environment, it also creates some security and privacy problems in cloud computing for sharing data. User's access request for data can itself reveal users privacy without considering whether he get the permission for accessing data. Also user storing data over cloud storage has no longer possession of data physically; it makes data integrity protection a hard task. So there is a necessity to develop a system which should protect user privacy and data integrity. Also it should be able to detect the fraud made to the shared data over a cloud server. So by considering the need of sharing data in cloud computing environment we have designed a system which address the above discussed security problems related to user's privacy and data integrity, our system protect user privacy by sending anonymous request when user requests other user's data for sharing over cloud storage. To share data with users proxy re-encryption is applied by cloud server. Attribute based encryption is provided so that user can only controls its own data fields. System also checks user data for its correctness by acting as a third party auditor (TPA). So our system provides a secure solution for sharing data over cloud storage.

2. RELATED WORK

A shared authority based privacy preserving protocol [1] which enables shared access authority to cloud users by using anonymous access request matching mechanism. Attribute based access control is used which enables user to access only its own data fields. Proxy re-encryption scheme is used by cloud server to facilitate data sharing between multiple users.

A secure cloud storage system which supports a public auditing with privacy preservation is proposed in [2]. Third Party Auditor (TPA) is available to verify user's private data for its integrity. TPA also be able to do audits for more than one users at same time and efficiently. Homomorphic linear authentication scheme (HLA) and Message authentication scheme (MAC) are used to verify data integrity.

An anonymous ID assignment based data sharing algorithm (AIDA) scheme for multiparty oriented cloud and distributed computing systems is proposed in [3]. In this scheme secure sum data mining methods are used to develop an integer data sharing algorithm. It also uses a variable and unbounded number of iterations for anonymous assignment. It works on Sturm's theorem and Newton's identities for data mining methods. Algorithm scalability is improved by using distributed solutions of some polynomials over finite fields. To detect statistics of the necessary number of iterations Markov chain representations are used.

A MONA (Multi-owner Data Sharing Secure Scheme) for dynamic groups in the cloud applications is proposed in [4]. With the use of MONA, user can share his data securely with other users via untrusted cloud and also supports to dynamic group interactions. In this data sharing scheme, a new user who granted access is able to decrypt data files without pre-contacting with data owner. A user revocation is performed with the use of revocation list. Secret keys of the other remaining users are not updated in revocation list in the process of revocation of one user. Any user in the group can uses cloud resources anonymously. This is decided by applying access control. Only group manager is able to reveal true identity of user for dispute arbitration. In this scheme encryption computation cost and overhead of storage is not related to the amount of users.

A distributed storage integrity auditing mechanism scheme to improve secure and dependable storage services in cloud computing [5]. To accomplish this, the Homomorphic token and distributed erasure coded data is introduced. The scheme allows users to make audit of the cloud storage. For this the communication and computation cost is kept low. The auditing results ensures the correctness of cloud storage. It also supports to dynamic outsourced data operations. It is shown that the scheme can recover quickly against malicious data modification attacks, server colliding attacks and Byzantine failure, to enhance the weakness of symmetric key cryptosystem in public clouds.

A broadcast group key management (BGKM) is proposed in [6] and it shows that, user do not need realize public key cryptography, and can dynamically generate the symmetric key in the process of decryption. According to this, attribute based access control scheme is developed so it can achieve that user is able to decrypt the data iff its attribute of identity match the content provider's policies. Fine grained algorithm applies Access Control Vector (ACV) to assign secrets to users depend on the identity attributes and allow users to derive symmetric keys based on their secrets and other public information. An advantage of BKGS is that when there is need for adding or revoking users and updating access control policy.

In above mentioned works, different security related problems are addressed that can affect data sharing in cloud. However users access request related privacy and data integrity issues are not given simultaneously. So here we have integrated these issues together and designed a system which can preserve user's privacy at the time of sharing data over cloud and also considering problems related to user's data integrity.

3. PROBLEM STATEMENT

The aim is to design a system which gets shared access authority by anonymous access request by considering the user security and privacy issues and realizes that user is able to only access its own data fields, share its data among multiple users by using proxy re-encryption. To verify data integrity auditing functionality technique is applied.

4. PROPOSED SYSTEM

4.1 System Model

The architecture of proposed system for storing data over cloud as shown in Fig-2. It consists of 'n' number of users, a cloud server or cloud storage (CS) and cloud storage system which acts as middleware between cloud server and cloud user. Users are able to perform operations such as login to system, upload data to cloud server by using Cloud Storage System, Send request for accessing other user's data by using cloud storage system etc. Cloud server (CS) stores user data in to a cloud storage it has. Main part of the architecture is cloud storage system. It performs the functions for user such as maintain the users database, authenticate the user, uploading user data to cloud server, anonymous access request matching for sharing the data, check the user data for its integrity etc.

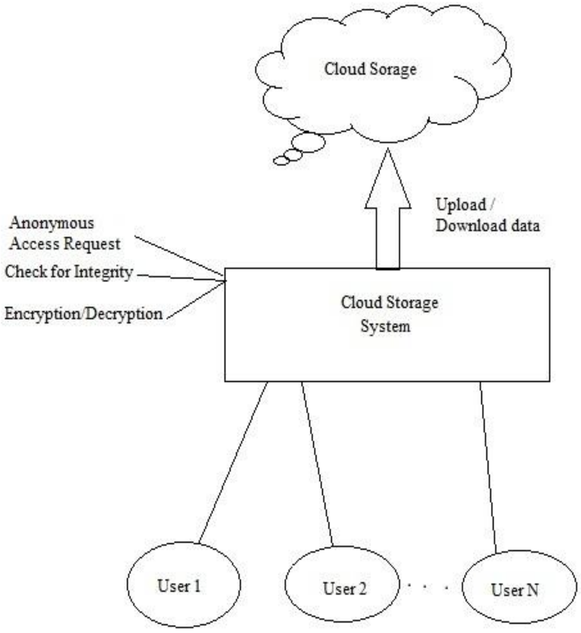

Fig -1: System Architecture

4.2 Threat Model

There is no any trust relationship between cloud server and users. Cloud server is semi-honest and curious and is considered as entity that follows strict protocol procedure. Cloud server may attempt to access users private data. It shows that cloud server is under the supervision of its cloud provider, and may have interest in users' private data. Other users also have interest in each other's data fields so they can also try to learn their data.

4.3 Design Goals

For effective utilization our system should achieve following security measures as follows,

- Anonymity: It guarantees that user get shared access authority of other users data without revealing the identity.
- Attribute based access control: It ensures that each user can only get access to its own data fields.
- Proxy re-encryption: It ensures that multiple user can share data among themselves.
- Data auditing: it ensures that system checks user data for its correctness without retrieving the whole copy of the data and without the additional burden on the cloud server.

4.4 Algorithms

We have used traditional cryptographic algorithm for encryption and decryption of user data before uploading/downloading to a cloud server. In addition to this we have used following algorithms

- K-Anonymity: K-Anonymity algorithm is the algorithms used for partially hide the user data. In our system we are using this algorithm for hiding user's personal information when he sends the data access request to other users so the user privacy is protected in getting shares access authority.

In addition to this we have used MD5 algorithm for generating signatures for files which are stored over cloud server. We also used Pseudo Random Number Generation algorithm for generating random keys for encryption. SOAP protocol is used to make connection to cloud.

5. PERFORMANCE ANALYSIS

We implemented our system by using C#.net technique and visual studio 2010 on windows system with intel core i3 processor. We have evaluated following results for the developed system.

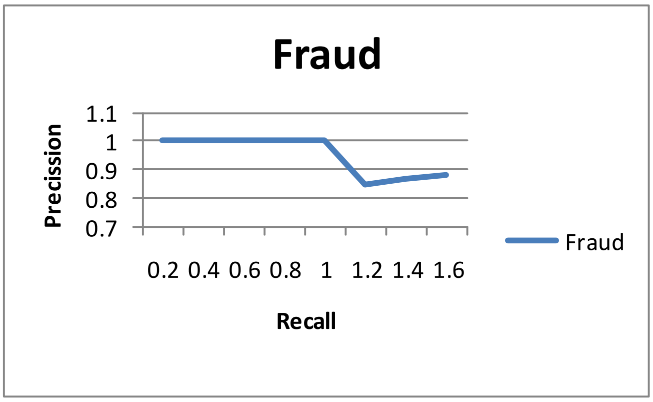

Chart -1: Number of frauds detected and number of frauds expected

Above chart-1 shows that the number of frauds detected and number of frauds expected in the system. System check for the fraud when user downloads the file from cloud server. System then performs the integrity check and detects fraud.

6. CONCLUSION

In this paper, we have described a cloud storage system which encourages users to share their data securely over cloud server without revealing their privacy. A system also checks the user data store on to the cloud serer and preserve user's data integrity. Overall our system preserves user privacy and data integrity of user data while sharing data in a cloud environment and facilitate a secure way for sharing data on the cloud server. So our system ensures that user's privacy and data integrity will be preserve. Our system will be applicable where there is use of cloud computing.

REFERENCES

[1]. H. Liu, H. Ning, Q. Xiong and L.T. Yang, "Shared Authority Based Privacy Preserving Authentication Protocol in Cloud Computing," IEEE Transactions on PARALLEL AND DISTRIBUTED SYSTEMS VOL:PP NO:99 YEAR 2014.

[2]. C. Wang, S.S.M Chow, Q. wang , K Ren and W. Lou,"Privacy-Preserving Public Auditing for Secure Cloud

Storage," IEEE Transactions on COMPUTERS, VOL.62, NO.2, FEBRUARY 2013.

[3]. L. A. Dunning and R. Kresman, Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[4]. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed systems.[online]ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnu mber=6374615, 2012.

[5]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing,Vol.5, no. 2, pp. 220-232, 2012.

[6]. M. Nabeel, N. Shang and E. Bertino, "Privacy reserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, [online] ieexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.

BIOGRAPHIES

Mr. Manoj Shantaram Tore received the B.E. degree in In Computer Engineering from University of Pune, in 2012. Currently he is pursuing Master's degree in Computer Engineering from Amrutvahini college of Engineering, Sangamner under University of Pune. His areas of interest are network Security and cloud computing. He is currently working in the field of Network security and Cloud computing.

Prof. S. K. Sonkar received the Master degree in Computer science and Engineering from SRTMU Nanded. He is currently pursuing the Ph.D. degree in computer science from University of Pune. He is presently working as Assistant Professor in Dept. of Computer Engineering in Amrutvahini college of Engineering, Sangamner, India. His current research interests include network security and Cloud Computing.