Secure Big Data Storage and Sharing Scheme for Cloud Tenants Using Trapdoor Function

Rashmi N. G[1] and Shrinivasa Naika C.L[2]

[1]*Student, Department Of Computer Science & Engineering, University BDT College of Engineering, Davanagere, India*
[2]*Assistant Professor, Department of Computer Science & Engineering, University BDT College of Engineering, Davanagere, India*

***Abstract*—Cloud computing is one of the most rapidly growing area which provides flexible, elastic and on- demand storage services for users. As cloud storage are growing rapidly data confidentiality, integrity and security in cloud storage system are always cause of concern. They are subject to attacks, modification and sometimes they even get stolen from storage system as our traditional security mechanisms doesn't provides enough security to our data. We are proposing new methodology where the mapping of big data are protected using trapdoor function and further we provide binary key encryption to every block of data.**

***Index Terms*—big data challenges, cloud computing**

I. Introduction

Big data is set of data which are beyond the ability of commonly used software systems to store, manage, and process within a tolerable elapsed time, they are ranging from terabytes to many petabytes. A data Centre mainly responsible for storing and processing of big data and those data are used for future scientific endeavors, Many IT industry are building their own data Centre to accommodate huge data. Consequently, large amounts of data requires security while processing and modification, as these data are very crucial for any organization we need to provide security at micro level in cloud storage.

Cloud storage system consist of many licensing and delivery models such as Software as a service , Platform as a service and Infrastructure as a service , They provides different services to customers as service on demand. These data services as provided over internet to clients from cloud storage media at different places, Users can have access to data from different locations with security intact as they are getting accessed from different location. SaaS provides software services.

In the proposed scheme, Data blocks are divided into multiple blocks of messages where each block have different data which will be stored in cloud storage. When data blocks are stored in cloud they will get encrypted using encryption keys, After storing the data blocks can be shared with authorized users.

II. Literature Survey

Data security is practice to protect data from unauthorized access and ensure privacy while protecting personal or corporate data. In a distributed environment, datasets are located in different data center and therefore face challenges such as data security, privacy protection and authentication, Many scheme have been proposed in past but they cannot be applied on big data efficiently as those algorithms are costly in terms of time and space. The first scheme is encryption which uses mathematical algorithms to scramble data into unreadable text. It can only be decrypted by the user who have valid decryption key, this method uses full file-level encryption, this scheme provides good security but it introduces some challenges with respect to key management and thus causes low efficiency and more time consumption. The second scheme is application-level data encryption technology, This technology provides

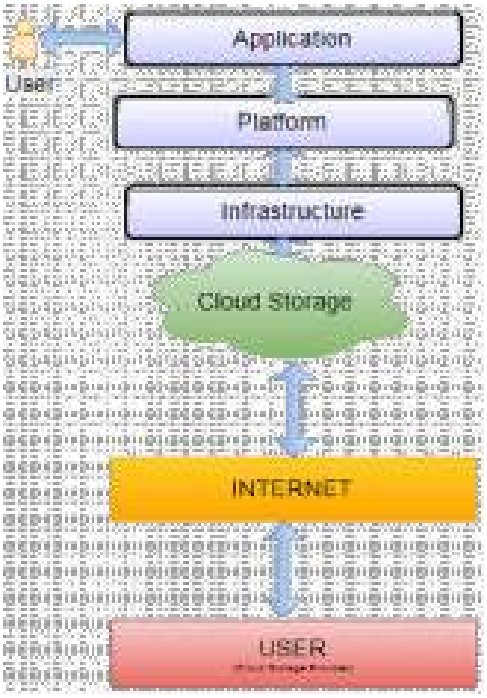

Fig. 1. Architecture of cloud storage

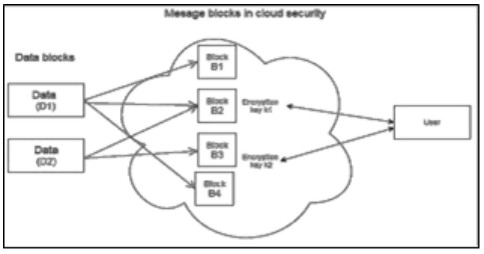

Fig. 2. Data in cloud storage system with trapdoor function

security when there is vulnerability in network level, it ensure that only certain users get to access the data through a particular application. This scheme will be very costly because it must maintain many parameters and data structures

III. Proposed System

As traditional security schemes are not efficient to protect big data we have come up with solution that prevents unauthorized access of data and meantime it will give secure access to the users as well. Today most of the user data are stored in cloud platform, People have variety of concern when they store their confidential on cloud storages. Undoubtedly, Privacy and security of personal data information is the most important concern for users. In order to make the big data of our users secure, we propose a secure cloud based storage system with binary encryption with trapdoor function. Each dataset will be separated into a sequence of n parts, where each part can be denoted by part i(i (1, n)) ,and they will be stored at m different storage providers, where each provider is identified as provider j(j (1,m)). These m storage providers may belong to one or more storage providers. so, when big data of a user's are stored, it will form unique storage path for the big data given as Mapping Storage Path=Data.((P1(M1,M2...Mr) (P2(M1,M2 ... MS);...(Pn(M1,M2...Mt); where, P denotes the storage provider, and M denotes the physical storage media. In the proposed scheme, our big data will be separated into multiple sequenced parts and then will be stored on different media. When users want to access their data then data from different part will be collected and clients gets access have data as one. these is very crucial because this protect our data from getting stole by any means, Further we use more advance security mechanism to protect our data. These data are classified into public data and confidential data.

We are going to introduce trapdoor function with binary encryption but prior to describing our proposed scheme we will introduce trapdoor function. A trapdoor function is a function that is easy to compute in one direction but difficult to compute in other and some piece of information can be made hard direction much easier. This can be explained as A can easily compute the encryption of his message using B's public key, but it will be very hard for C to reverse this process. B can use private key to read A's message Trapdoor function will provide strong security to our system along with that we propose proxy re-encryption scheme, a proxy re-encryption schemes allows third parties to alter cipher text which is encrypted by one party, so that it may be decrypted by another. These scheme are applied when user want to share his data at that time he have to send re-encryption key to the storage server after that server will re-encrypt the message and for authorized users this will increase data confidentiality and enhances the data forwarding function. Our proposed scheme have lower transmission failure probability and mainly focused upon sharing of confidential data, our scheme protect the privacy and confidentiality of data and they are remains non-accessible to unauthorized users.

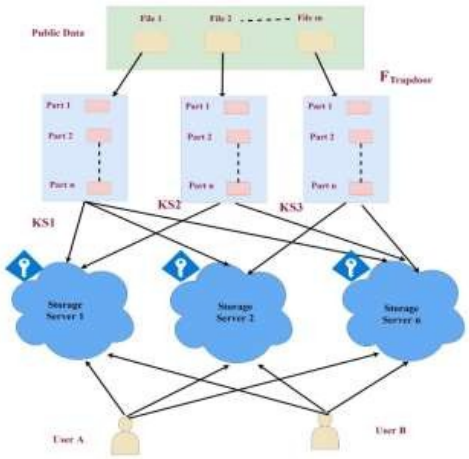

Fig. 3. Data delivery mechanism in the cloud storage

IV. Simulation

To describe the simulation we design a procedure to establish communication key between different users, which used to establish communication among user for sharing bid data. We use different parameters to describe the identity element of system, Zq to denote group under modulo q.
Algorithm:

The procedure of establishing communication key between user A and other cloud user, for example B

1) Tenant A computes parameter Y_A: Choose $X_A < q$
2) $Y_A = \eta^{XA}$ mod q. User B computes parameter.
   Y_B: Choose $X_B < q$
   Compute $Y_B = \eta^X B$ mod q.
3) Tenant A encrypts Y_A, ID_A and ID_B using IBE algorithm and then send to B:
   Encrypt (Y_A,ID_A and ID_B) $\rightarrow B$
   User B encrypts Y_B, ID_B and ID_A
   using IBE algorithm and then send to B: Encrypt (Y_B, ID_B and ID_A) $\rightarrow A$

In Simulation, we evaluate the efficiency and data storage robustness of proposed scheme and traditional scheme using different scenarios. In first simulation scheme, big data transmission overhead of traditional scheme will be compared with proposed scheme with same data size; we test with these condition 5 times and the results are shown in diagram. In second simulation we check the data availability in serving data to cloud clients, the traditional schemes may have unavailable during failure time but newly proposed scheme will be robust as data are divided into multiple parts.

V. Conclusion

In this paper, we have to propose the new method for constructing Secure Big Data Storage and Sharing Scheme for Cloud Storage using trapdoor function. as big data requires large space and time our proposed model avoids this by splitting data into multiple blocks and protect it with trapdoor function. We analyzed the proposed scheme with respect to security and efficiency and all results show that proposed scheme is effective and feasible to protect the big data. Future

researches might consider in future such as using the indexing method to split the files and stored in the cloud using meta search algorithm.

REFERENCES

[1] H. Y. Lin and W. G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 995-1003, June 2012.

[2] K. Zhang, J. Kong, M. Qiu and G.L Song, "Multimedia Layout Adaptation Through Grammatical Specifications," in *ACM/Springer Multimedia Systems*, vol. 10, no. 3, pp.245–260, 2005.

[3] Q. Liua, G. Wang and J. Wu, "Secure and Privacy Preserving Keyword Searching for Cloud Storage Services," in *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 927-933, May 2012.

[4] A. Cidon, R. Stutsman, S. Rumble, S. Katti, J. Ousterhout and M. Rosenblum, "MinCopysets: Derandomizing Replication in Cloud Storage," in *Networked Systems Design and Implementation*, Stanford University, 2013.