ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

ENHANCING DATA SECURITY IN CLOUD STORAGE

Sunita Sharma[1], Amit Chugh[2],Ajay Kumar[3]

M.Tech. Student, Dept. of CSE, Lingayas University Faridabad, Faridabad, India[1]

Assistant Professor, Dept. of CSE, Lingayas University Faridabad, Faridabad, India[2]

Software Engineer, Aricent Group, Gurgaon, India[3]

Abstract: We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. We envision several possible directions for future research on this area. To ensure the correctness of user's data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. To ensure the security of data, we proposed to use DES (Data Encryption Standards) algorithm. In present paper we have given a working architecture of Cloud data security using DES algorithm.

Keywords: DES Algorithm, Cloud Service Provider, Third Party Auditor (TPA), Cloud Authentication Server

1. INTRODCTION

DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession.

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such. The key is nominally stored or transmitted as 8 bytes, each with odd parity. According to ANSI X3.92-1981, section 3.5: t in each 8-bit byte of the *KEY* may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16, 64 are for use in ensuring that each byte is of odd parity.

Expansion — the 32-bit half-block is expanded to 48 bits using the *expansion permutation*, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 * 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.

Key mixing — the result is combined with a *subkey* using an XOR operation. 16 48-bit subkeys — one for each round — are derived from the main key using the *key schedule* (described below).

Substitution — after mixing in the sub key, the block is divided into eight 6-bit pieces before processing by the *S-boxes*, or *substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table.

Permutation — finally, the 32 outputs from the S-boxes is rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, each S-box's output bits are spread across 6 different boxes in the next round.

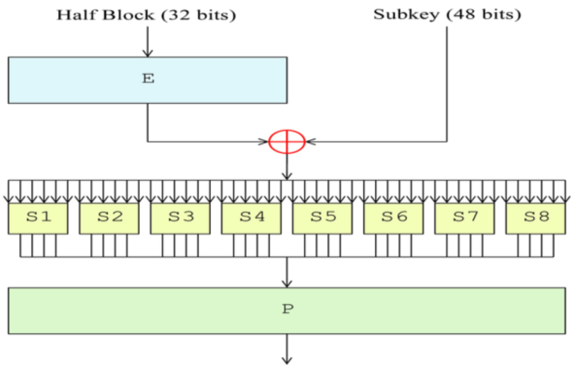

Figure 1

II.RELATED WORK

Storing data into the cloud, gives great convenience to users as they don't have to care about the complexities of resource management. Cloud pioneers like Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2), gives huge amounts of storage space and customizable computing resources. Due to this, responsibility of local machines for data maintenance is eliminating. As a result, cloud users are at the mercy of their service providers for the availability and integrity of their data, downtime of Amazon's S3 is an example. From the perspective of data security, which has always been an important aspect of QOS(quality of service), Cloud Computing inevitably poses new challenging security threats for number of reasons. Some of theseare :

i. Traditional cryptographic primitives for the purpose of data security protection can't be directly adopted, due to this user control lose on data on cloud.
ii. Ensure storage correctness under dynamic data update(can be insertion, deletion and modification) of stored data.
iii. Deployment of Cloud Computing powered by data centers running in a simultaneous, cooperated and distributed manner.

Analyzing the above threats we have constructed a system which can handle these threats. System Consist of different components and some of these components ensures safety from above threats. Short description of system components are :

A. Client component:

In this part, client sends the query to the cloud server. Based on the query the server sends the corresponding file to the client. Before fulfilling the request of client, client authorization step is done at cloud server. During authorization, Cloud server checks the client name and password. If credentials are proper it searches the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative path to intruder.

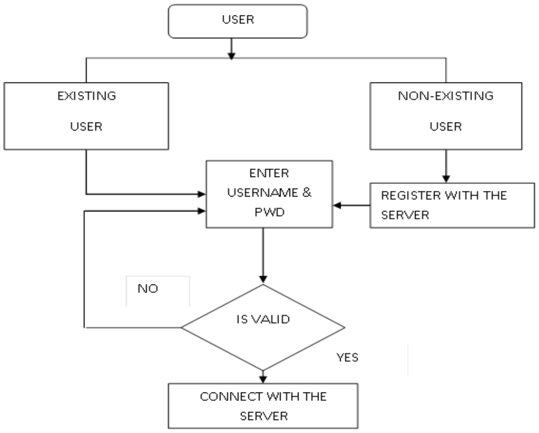

Figure 2

B. System component:

Network architecture for cloud data storage is illustrated in above diagram. Three different network entities can be identified as follows:

• User:

Users, who stores data in the cloud and rely on the cloud for data computation. Cloud consist of both individual consumers and organizations.

• Cloud Service Provider (CSP):

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems. It is the central entity of cloud.

• Third Party Auditor (TPA):

An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

E. Cloud data storage component:

This component refers to the actual process of data storing in cloud. User stores his data through a CSP into a set of cloud servers. For retrieving data, user interacts with the cloud servers via CSP. In some cases, user may need to perform block level operations on his data, it can be achieved only after retrieval of data from cloud. Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

F. Cloud Authentication Server component:

Cloud Authentication Server (CAS) functions as any authentication server (AS) would, with a few additional behaviors added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The CAS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the CAS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request

G Unauthorized data modification and corruption component:

One of the key issues is to effectively detect any unauthorized data modification and corruption. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance.

H Data security component:

Data security component is responsible for storing and retrieving secure data. Here we have used DES technique for storing and retrieving secure data. This is main component enabling security in our system.

I. Adversary component:

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, untrusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors. On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete user’s data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of adversary with different levels of capability:

Weak Adversary*:* The adversary is interested in corrupting the user’s data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user. Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

Working Architecture of System:

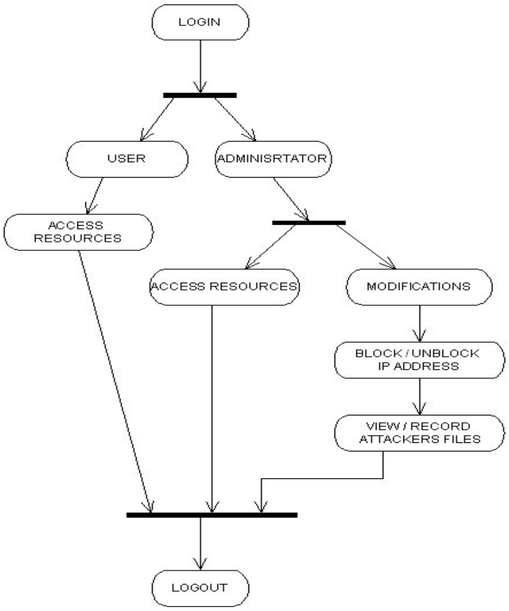

Figure3

IV. CONCLUSION

In this paper, we have discussed working system design for data security in cloud storage. we discussed architectural components for providing data security at both levels (User and Administrator). To ensure the correctness of user's data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append operations. For data security we have used DES algorithm, which lets data stored in the database as cipher text and on request data is available in the required format. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). We have used DES algorithm with erasure-correcting technique for providing data security with integrity.

REFERNCES

[1]http://en.wikipedia.org/wiki/Data_Encryption_Standard

[2] K.S.Suresh,ProfK.V.Prasad ,” Security Issues and Security Algorithms in Cloud Computing”, Volume 2, Issue 10, October 2012

[3] Neha Jain, Gurpreet Kaur,” Implementing DES Algorithm inCloud for Data Security”, VSRD-IJCSIT, Vol. 2 (4), 2012.

[4] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws. amazon.com, 2008.

[5] N. Gohring, “Amazon’s S3 down for several hours,” Online Adown for several hours.html, 2008.

[6] A. Juels and J. Burton S. Kaliski, “PORs: Proofs of Retrievability forLarge Files,” Proc. of CCS ’07, pp. 584–597, 2007.

[7] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” ProcofAsiacrypt ’08, Dec. 2008.

[8] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theoryand Implementation,” Cryptology ePrint Archive, Report 2008/175,2008, http://eprint.iacr.org/.

BIOGRAPHY

Sunita Sharma has received her Master degree in Computer Application (MCA) from M.D. University, Haryana, India. Currently she is pursuing M.Tech. (Computer science) from Lingaya’s University. She has around 3 years of teaching experience. Her areas of interests include Artificial Intelligence, Networking, data mining etc.

Mr. AmitChugh is working as an Assistant Professor in the School of Computer Science at Lingaya’s University, Faridabad Haryana, and India. He has authored 15 papers and his areas of interests include Artificial Intelligence, Cognitive Science, Networking, Brain Computer Interface, and Image & Signal Processing.

Mr. Ajay Kumar is working as software engineer at Aricent Group, Gurgaon(India). His areas of interests include Artificial Intelligence, Java Programming, Networking and Telecommunication.