International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 1667–1676

"Data Storage & Security in Cloud Computing"

Shradha Parmeshwar Awatari
Dr. Sachin Chaudhari
Prof. Monali Gulhane

Department of Computer Science & Engineering
M. Tech Jhulelal Institute of Technology, Nagpur, Maharashtra, India

Abstract

Cloud computing is now days emerging field because of its performance, high availability, low cost. In the cloud many services are provided to the client by cloud. Data store is main future that cloud service provides to the companies to store huge amount of storage capacity. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing.. The main objectives of this paper are, 1) To prevent Data access from unauthorized access, it propose a distributed scheme to provide security of the data in cloud .This could be achieved by using homomorphism token with distributed verification of erasure-coded data. 2) Proposed scheme perfectly stores the data and identifies the any tamper at the cloud server.3) And also performs some of the tasks . like data updating, deleting, appending.

Keywords:*Data storage & cloud Computing, Cloud Computing, Cloud Storage,Cloud Environment, Cloud Security*

INTRODUCTION

This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users.

The pioneer of Cloud Computing vendor,(example) Amazon S3 is storage for the Internet. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It also allows developer to access the highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. From the viewpoint of data security, which has always been an important aspect of quality of service, Cloud Computing unavoidably poses new challenging security threats for number of reasons.

- Unauthenticated person don't attack the
- Authorized file Avoids Collusion attacks
- Malicious data modification attack
- Dynamic Data operation
- Identification tamper server

Cloud computing is the most demanding and emerging technology throughout the world. Cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and google have implemented the "CLOUD" and have been using it to speed up their business. Cloud computing has given a new dimension to the complete outsourcing arena (SaaS, PaaS and IaaS) and they

ISSN: 2233-7857 IJFGCN

provide ever cheaper powerful processor with these computing architecture The major thing that a computer does is to store in the available space and retrieve information whenever requested by the authenticated user

Fig.1. Results of IDC survey ranking security challenge

Related Work

The Internet began to grow quickly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent year has dramatically enhanced the stability of variour application services available to uses through the Internet, thus marking the beginning of cloud Computing network services many organization tried to enhance for their security constraints, for their secure database, f or their web application but they have not achieved a high-level security for their organizations. Data integrity quality of correctness, completeness, wholeness soundness and compliance with the intention of the creator of the data. It i achieved y preventing accidental or deliberate but unauthorized insertion, modification or destruction o f data in a database. Ensuring the integrity of the data really me answered that it changes only i n response to authorized transactions.(see Fig.1) given state confirm that the “Security” is the main Challenge in Cloud Computing For example IDC recently conducted a survey of 244 IT executives/CIOs and their line- of-business (LOB) colleagues to gauge their opinions and understand their companies’ use o f IT cloud services. Security ranked first as the greatest challenge or issues of cloud computing.
The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any prove that passes a verification . Juels and Kaliski [3 proposed a scheme called “provable data possession” (PDP) mod l for ensuring possession o f file on un trusted storages. Their scheme utilized public key based homo orphic tags f or auditing the data file, thus providing public verifiability.

J.C.Mogul;[4]proposed a scheme called “Auditing to Keep online Storage Services Honest” The need for auditing to support an online service-oriented economy. They highlight issues around both internal and external auditing. This paper [2][4][9],allow TPA to audit the cloud data storage without demanding user’s time feasibity (or) resources. The proposed method provides public key verification for secured storage and investigate the problem of fine - grained data error Localization in the c loud.

ISSN: 2233-7857 IJFGCN

3. Problem Statement

From the perspective of data security, which h has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

Data stored o n cloud serve s is not completely secure from infection**.** While popular cloud services such as Google Do s are equipped with virus scanning software, there is still the possibility of an internal or external attack affecting your data.

The data stored in the cloud may be frequently
updated by the users, including insertion, deletion, modification, appending, recovering, etc. To ensure storage correctness under dynamic data update, distributed protocol is used.

A descriptive architecture for se cure data storage is illustrated in(see Fig .2) Data storage in a cloud is a process where the owner stores his data, files and applications through a Cloud Storage Provider (CSP) into a set of cloud servers. At the time of file storage, security key is used to secure the file from unauthorized access and then safely stored in the cloud. User who likes to access the file from cloud needs the security key to retrieve the file. User sends
request to the owner and retrieves the file from the c loud after security key send by the owner. File can't be accessed by any Unauthorized per on or person who entering unmatching security key. For additional security, blocking IP address of the system those who illegally trying to access the file.
Data storage in a cloud is a process where the owner stores his data

This paper proposes using homomorphic token & verification of erasure-coded the current research provides cloud data security along with minimizes the redundancy.

The distributed protocol in our work future provides the localization of data error. Which only provides binary results about the storage state across the distributed service in predecessors.

Operations like Update, delete and integrity are also provided in the proposal methods.
Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server Collusion attacks.

4. Secure Data Storage in Cloud

In cloud storage system, companies stores their data in the remotely located data server. Accordingly, correctness of the data is assured. Even though sometimes unauthorized person may modify or delete the data which leads to server compromise and/or random Byzantine failures. Because it can be the first step for fast recovery of the storage errors. The cloud storage systems propose an effective and flexible distributed scheme with explicit dynamic data support for file distribution across cloud servers. By computing homomorphic token using universal hash function [7] which can be perfectly integrated with the verification of erasure-coded data. As well as it identifies misbehaving servers. Finally, the procedure for file retrieval and error recovery based on erasure-correcting code is outlined.

4.1Token correctness

It achieves assurance for data storage correctness and data error localization, using pre-computed token. Before sharing file distribution using pre- computes a certain number of shortest verification token are generated that will ensure security for a block of data in a file in cloud storage. When the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of

ISSN: 2233-7857 IJFGCN

randomly generated block indices. After getting assurance of the user it again asks for authentication by which the user is confirmed to be the authenticated user. Upon receiving assurance, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens pre-computed by the user. All servers operate over the same subset of the indices

The requested response values for integrity check must also be a valid codeword determined by a secret matrix. Suppose the user wants to challenge the cloud server's t times to make sure the correctness of data storage. Then, he must pre- compute t verification tokens for each function, a challenge key and a master key are used. To generate the i th token for server j, the user acts as follows the details of token Generations are shown in Algorithm 1.

Derive an arbitrary value i and a permutation key based on master permutation key.
Calculate the set of randomly-chosen index.

Calculate the token using encoded file and the arbitrary value derived.

Algorithm 1 Token Pre-computation Block of data is represented as l;

No. of .blocks is denoted as n;

Let f be the function and t be the token ; Index per proof is denoted as r;

Generate M_k and $\mathbf{C}_k$;

For point G (j); j->1, n execute

/*j server position*/

For round i->1, t execute

/*i block index*/

Derive i = f (i) and k (i) from master key.Compute v(j)

End for

End for

Store all the vis locally.

End procedures

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented as follows;

ISSN: 2233-7857 IJFGCN

A. Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) [6] is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation and sixteen Feistel rounds [7]. Each round uses a different 48-bit round key generated from the cipher key. DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds

.Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text.

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

B. RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adelman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Key Generation	
Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

ISSN: 2233-7857 IJFGCN

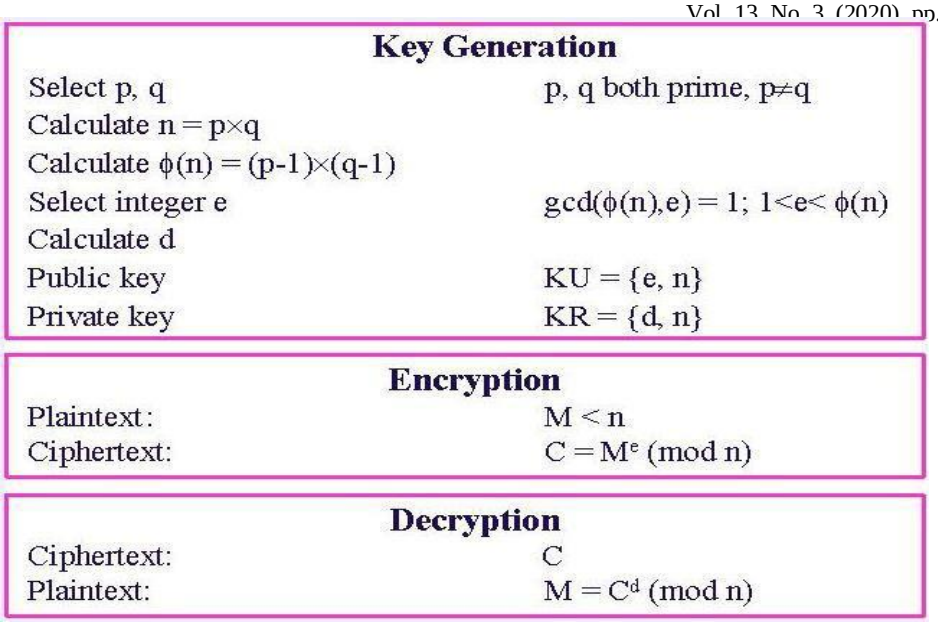

Figure 1. RSA Algorithm

RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at Encryption
$C = M^e \bmod n$
And at decryption side
$M = C^d \bmod n$.

Where n is a very large number, created during key generation process.

DES algorithm and RSA algorithm provides security in cloud storage. In existing systems only single level encryption and decryption is applied to Cloud data storage. Cyber criminals can easily cracked single level encryption. Nowadays Cyber Criminals can easily access data storage. In Personal Cloud Storage important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task. We have proposed a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload data in Personal Cloud Storage. Uploading file DES and RSA Encoding schemes are used to encrypt data.

The steps of Multi-level encryption will be as follows:

- Upload data.
- Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block

cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The actual key used by DES algorithm for encryption is 56 bits in

ISSN: 2233-7857 IJFGCN

length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds

- DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially.
- The first level encryption is generated using DES algorithm
- Now apply RSA algorithm on encrypted output of DES algorithm to generate second level encryption.
- In RSA algorithm public key is used for encryption.
- Once the data is encrypted using RSA algorithm, it will be stored in Database of Cloud Storage.

The steps of Multi-level decryption will be as follows:

- DES and RSA algorithms are used to decrypt data.
- First apply the RSA algorithm (decryption scheme) using private key. This algorithm will generate first level decrypt data.
- Now apply the DES decryption algorithm on first level decrypt data.
- DES decryption algorithm uses the same 56 bit length key for decryption.
- DES algorithm of decryption will generate Plain text.

In Our proposed algorithm, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. And same Process takes place for decryption using DES and RSA algorithms. Means we applied multilevel Encryption and Decryption to provide security for cloud storage data.

5. Implementation

5.1 Secure Software Development Life Cycle

Phase1.Investigation**:**Define project processes and goals, and document them in the program security policy.

Phase2.Analysis: Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.

Phase3.Logical design: Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

Phase4.Physical design: Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

ISSN: 2233-7857 IJFGCN

Phase5.Implementation: Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

Phase6.Maintenance: Constantly monitor, test, modify, update, and repair to respond to changing threats.

5.2 Main Modules

5.2.1 Client Module

The client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search 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 that intruder. Using screen shown in fig.3.

5.2.2 System Module

User

Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud Service Provider (CSP)

The Security Development Lifecycle (SDL) is a software development security assurance process consisting of security practices grouped by seven phases Investigation, Analysis, Logical design, Physical design, Implementation, Maintenance.

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

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.

ISSN: 2233-7857 IJFGCN

5.2.3 Cloud Data Storage Module

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data.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 that 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. Using screen shown in Fig.4.

5.2.4 Cloud Authentication Server

The Authentication Server (AS) functions as any 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 AS 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 AS 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. Using screen shown in Fig.5.

5.2.5 Misbehaving server model

When the user enters into cloud server and the user will start to access the file, but at the same time an unauthorized user enters into the cloud server without the proper authentication to the cloud server the particular IP address will be noticed and it makes some attention to the cloud owner. Using screen shown in fig.6.

IV. CONCLUSION

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the technique for data secure by converting the data into coded or non readable forms. But the existing cryptographic Algorithms are single level encryption algorithms. Unauthorized person can easily cracked single level encryption. Hence system which uses multilevel encryption and decryption it provides more security for Cloud Storage.

As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using

ISSN: 2233-7857 IJFGCN

References

[1] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, Security", CRC Press 2009 by Taylor and Francis Group, LLC.
[2] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc.of Asiacrypt '08, Dec. 2008.
[3] G.Ateniese. R. D. Pietro ,L.V.Mancini and G. Tsudik, "Scalable and Efficient Provable Data Possession,"Proc of Securecomm'08.
[4] M.A Shah, M.Baker, J.C.Mogul, "Auditing to Keep Online storage services Honest,"Proc 11th USENIX Workshop on Hot Topics in Operating Systems(HOTOS'07). pp. 1–6, 2007.
[5] T.S.J.Schwarz and E.L.Millerds, "Store, Forget, and check: Using Algebraic Signatures to Check Remotely administered Storage,"proc.of ICDCS'06, pp. 12–12, 2006.
[6] Case study: http://eyeos.org/ cloud desktop

ISSN: 2233-7857 IJFGCN