Enhancement of a Novel Secure Dependable Data Storage & Privacy in Cloud Network

Prof. B. Anuradha, V. Nithya

Abstract— **There is a tremendous development in networking technologies with on demand quality of services in cloud environment. Cloud computing is the delivery of computing as a service rather than a product, shared resources such as software, hardware and infrastructure are provided to computers and other devices as a metered service through a network. Cloud computing provides computation, software, storage resources and data access, in which cloud users are without knowing to the location and other details of the computing infrastructure. In cloud research study reveals that there is a problem in security management and privacy services. To overcome this privacy problem there is a new technique known as multifactor authentication, and trusted third party auditing. For avoiding security issues there is a technique as erasure correcting coded data. That is error detection and correction (identification of misbehaving server). In this paper we propose secure dependable storage with the help of key server concept. This will be drastically reduced the communication and storage overhead as compared to the traditional replication-based file distribution techniques.**

Index Terms— **Data dependability, Data Dynamics, Data integrity, Security**.

I. INTRODUCTION

All Cloud computing is a process in which computing power, memory, infrastructure can be delivered as a service. A Cloud computing is a firm of network enabled services, guaranteed QoS, inexpensive computing infrastructures on demand with an easy and simple access. Cloud security is an emerging sub domain of computer security, network and information security. Security in cloud can be instrumented remotely by client where the data centres and protocols in the security objectives of the service provider are: i) confidentiality for securing the data access and transfer ii) auditability for checking whether the security aspect of applications has been tampered or not. Dimensions of cloud security have been totalled into three areas [1] like security and privacy, agreement and legal issues.

Cloud Computing is a technology that uses the Internet and central remote servers to maintain data and applications. It allows businesses and consumers to use applications without installation and access their personal files at any computer with internet access.

Cloud computing exposes the following key characteristics:

•Reliability is improvised if multiple redundant websites are used, which creates well designed cloud computing suitable for business continuity and disaster recovery.

•Scalability and Elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis real-time, without users having to engineer for peak loads.

•Cloud computing applications are easier to maintenance, because they do not need to be installed on each user's computer and can be accessed from different places.

•Virtualization technology allows servers and storage devices to be shared and utilization to be increased. Applications can be easily moved from one physical server to another.

Fig. 1 Cloud Computing

A. TPA

In order to unravel the problem of data integrity checking, many schemes are implemented under different systems and security models. In all works, great efforts are made to design solutions that meet various requirements: high scheme of efficiency, unbounded use of queries stateless verification and retrievability of data, etc. To consider the role of the verifier in this model, all the schemes are presented before fall into two categories: private auditability and public auditability. Even though schemes with private auditability can be achieved higher scheme efficiency, public auditability allows any one, not just the client (data owner), to be challenged the cloud server for correctness of data storage

Manuscript received Jan, 2014.

V. NITHYA, PG Scholar, IT Department, SNS COLLEHE OF ENGINEERING, Coimbatore, India,+917708443003,

B.ANURADHA, HOD/Assistant Professor, IT Department, SNS COLLEHE OF ENGINEERING, Coimbatore, India,

while keeping no private information. Then, clients can delegate the evaluation of the service performance to an independent TPA [2] [3], without devotion of their computation resources.

TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether the data stored in the cloud are indeed intact, which can be essential in achieving economies of scale for Cloud Computing. The released audit report should not only help owners to evaluate the risk of their subscribed cloud data services [4] [5] [6], but to be beneficial for the cloud service provider to improve their cloud based service platform .This public auditor will help the data owner that his data are secure in cloud. With the help of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand.

B. *AES ALGORITHM*

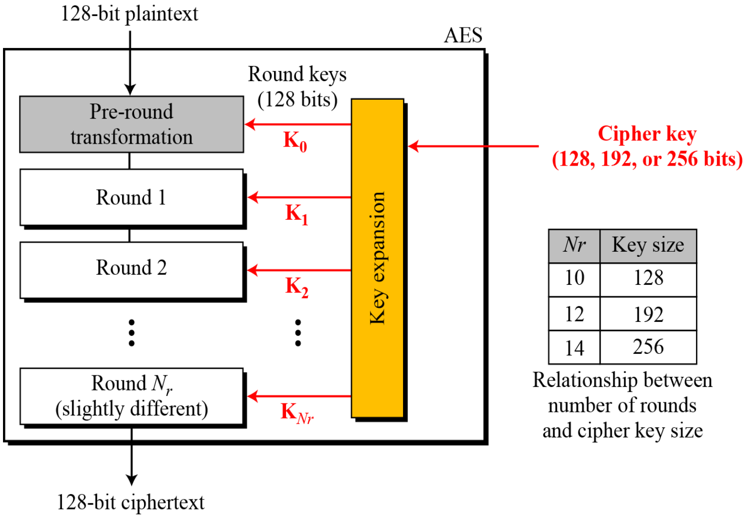
The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm [11]. It is used for secure and classified data encryption and decryption.

The AES has three fixed 128-bit block ciphers with cryptographic key sizes such as 128, 192 and 256 bits. the block size maximum is 256 bits, whereas, Key size is unlimited. The AES design built on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network.

The DES is replaced by AES with new and updated features:

- Block encryption implementation
- 128, 192 and 256-bit key lengths with 128-bit group encryption
- Symmetric algorithm require only one encryption and decryption key
- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation.

For Example [9][12], Amazon S3 Server Side Encryption employs strong multi-factor encryption. Each data object is encrypted with a unique key. As an additional safety measure, this key itself is encrypted with a regularly rotated master key. Amazon S3 Server Side Encryption uses one of the strongest block ciphers available 256-bit Advanced Encryption Standard (AES-256) -- to encrypt your data.



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Fig.2. General Design of AES encryption cipher (taken from [10]).

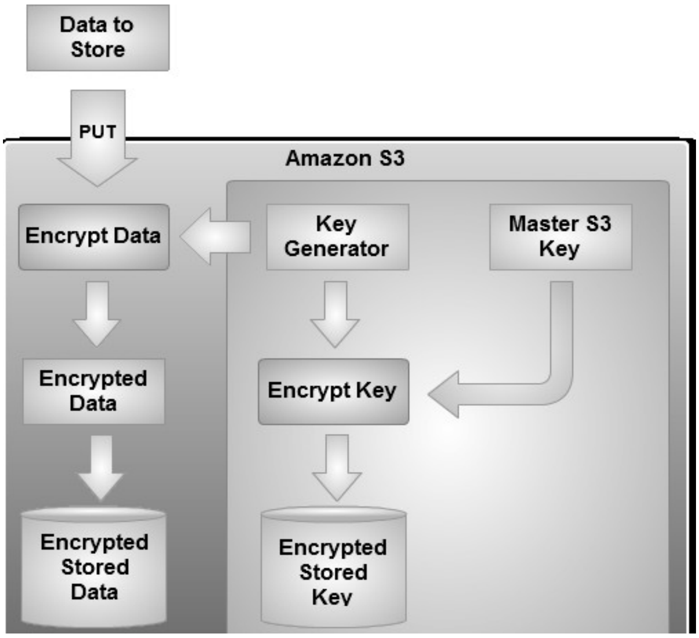


Fig.3. Amazon S3 Server Side Encryption (taken from [13])

II. PROPOSED WORK

A. *System Design*

While data stored in cloud server, the dependable data storage is used, whereas data will be stored in more than one server. User can upload their data files into CSP servers. All data blocks never stored in same server. That should be resided in different CSP server‘s location. CSP will encrypt the data blocks using key. Master server should aware of where that particular data block is to be present in which server.

When storing each file, user level authentication to be done. Then that will be password protected. So that others cannot ace

ss that files. But actual authorized user can view and edit their file without any burden.

Besides, User will be done dynamic data operation into the CSP. When delete operation one time password mechanism will be used. After a conformation from actual user the file will be deleted.

B. *Advantages of Proposed System*

- Space: Since Raptor codes require storage for the intermediate symbols, it is important to study their space consumption. Count the space as a multiple of the number of input symbols. The space requirement of the Raptor code is 1/R, where R is the rate of the pre-code.

- Overhead: The overhead is a function of the decoding algorithm used, and is defined as the number of output symbols that the decoder needs to collect in order to recover the input symbols with high probability, minus the number of input symbols. Measure the overhead as a multiple of the number of input symbols, so an overhead of , for example, means that $(1+\varepsilon)K$ output symbols need to be ε for example, means that $(1+\varepsilon)K$ output symbols need to be collected to ensure successful decoding with high probability.
- Cost: The encoding and decoding process cost is less.

C. *Ensuring Secure Cloud Data Storage:*

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. So that, the Storage Correctness of the data files being stored on the distributed cloud servers must be sure [2]. One of the key issues is to well detect any unauthorized data modification and corruption, probably due to server compromise and/or random Byzantine failures.Moreover, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks.

The procedure for file retrieval and error recovery based on erasure correcting code is also outlined.

D. *Dynamic Data Operation*

So far, Assume that F represents static data. This model may fit some application developments, such as scientific datasets and libraries [2]. But, in cloud data storage, there are many potential circumstances where data stored in the cloud is dynamic, like electronic documents, log files, or photos etc. Therefore, it is crucial to consider the dynamic situation, where a user may wish to perform various block-level operations of delete, update and view to modify the data file while maintaining the storage correctness assurance.

Since data do not reside at users' local site but at cloud service provider's address dynamic data operation can be quite challenging. Initially CSP needs to process the data dynamics request without knowing the secret key. On the other hand, users need to ensure that the entire dynamic data operation request has been faithfully processed by CSP. For any data dynamic operation, the user must first generate the analogous resulted file blocks and parities. This kind of operation has to be carried out by the user.

Besides, to ensure the changes of data blocks correctly reflected in the cloud address that the user also needs to modify the corresponding storage verification tokens to accommodate the changes on data blocks.

In other words, these verification tokens help ensure that CSP would correctly execute the processing of any dynamic data operation request. This would clearly be highly inefficient.

E. *Result and Discussion*

1) *Developing a Cloud Network with MFA*: Initially the basic network model for the cloud data storage is developed in this module. There are three different network entities that can be identified as follows: User: an entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers [7]. Cloud Server (CS): an entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter). Third-Party Auditor: an optional TPA has skills and abilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

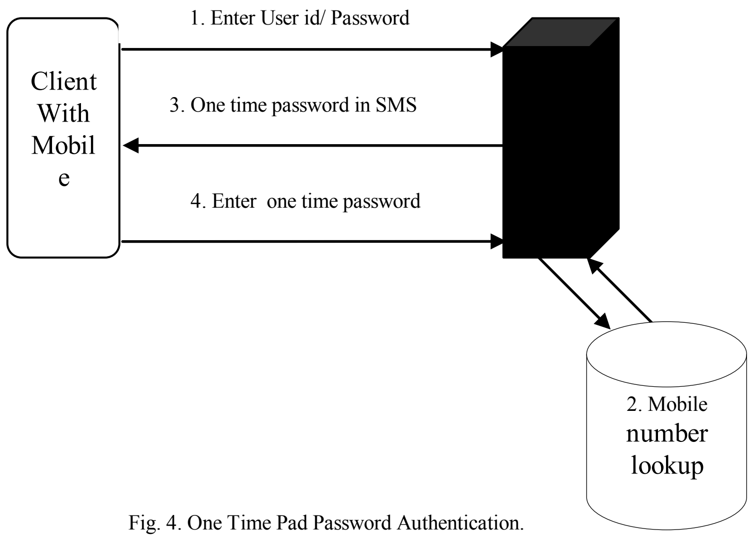

1. Enter User id/ Password
Client With Mobil e
3. One time password in SMS
4. Enter one time password
2. Mobile number lookup

Fig. 4. One Time Pad Password Authentication.

During login, client gives own user id and password. This input is encrypted to form digest and this digest sends to server side. At server side, stored password is encrypted and compared with the digest from client side. If both are same then client gets the authorization. But, if administrator with high privileges can decrypt the file which may cause unauthorized access to user data. Now a day, one of the strong authentication mechanisms is two factor authentications with one time pad password. Fig. 4 presents how a two factor authentication with one time pad mechanism is worked through mobile SMS.

2) Key Server Concept: To propose a practical application for private data management, which we name it as OWUR/W (owner-write-users-read/write) applications, where a data source protected with a node key in a key management tree can be shared with or managed by another party without compromising the security of the data encrypted with its child nodes' keys. Additionally, data can be updated not only by the data owner, but also by other legitimate parties. To be found that this scenario is very useful in outsourcing management.

Intuitively, want to realize that the encrypted data block associated with a node can be decrypted by multiple decryption keys where one of them is associated with the tree and can be utilized to generate its keys children's keys, while other decryption keys are only used to decrypt the data block stored in the node. Let us assume [9] two decryption keys (d1, d2), assigned to a node, where one of them is associated with the tree (let us assume that d1 is the key associated with the tree and is known to the manager only). Both decryption keys are associated with the unique encryption key, e. With d2, the user can decrypt the data block but cannot generate the decryption keys of this node's children. We believe that this method offers an additional privacy protection to the outsourced data.

Let us use a binary tree as an example [8] and (i, j) as an arbitrary node. Then the main construction contains four algorithms: key generation, encryption, decryption and key derivation.

Key generation: The decryption keys are denoted by (dij1, dij2), which correspond to (x1, x2) in the 2-degree polynomial defined above, where dij2= H (dij1).

For simplicity, we denote (dij1, dij2) = (d1, d2). The encryption key corresponding to (d1, d2) is e = (g0, g1, g2), where g0 = ga0 = gd1d2, g1 = ga1 = g-(d1 + d2), g2 = ga2 = g. For simplicity, we have omitted the subscripts of eij.

Encryption: The encryption algorithm takes as input a message M ε{0, 1}*the encryption key e, a random k ε Zq and a generator h ε Z*p and outputs a cipher text (c1, c2), where

$$C_1 \leftarrow (h_k.g0_k.g1k.g2k),\ C_2 = M*h_k \qquad (1)$$

Decryption: This algorithm takes as input the cipher text (c1,c2) and one of decryption keys d1 and d2, and outputs M * h_k can be computed from b1 * bdi 2* bd2i 3 , for i ε {1,2 }Thus, M can be computed as $M=C_2/h_k$ (2)

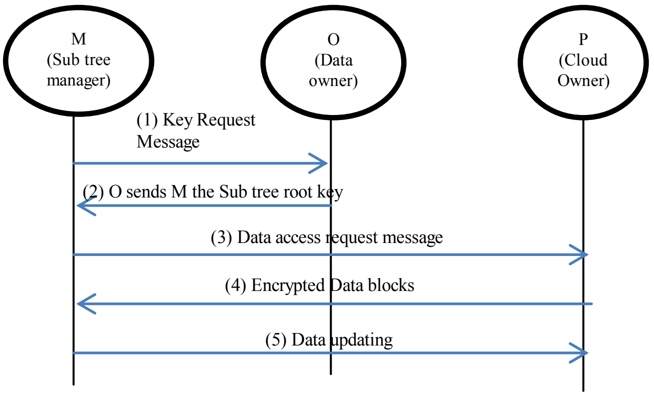

M
(Sub tree
manager)
O
(Data
owner)
P
(Cloud
Owner)
(1) Key Request
Message
(2) O sends M the Sub tree root key
(3) Data access request message
(4) Encrypted Data blocks
(5) Data updating

Fig. 5. (a). Secure Key Distribution Between User and Cloud Owner.

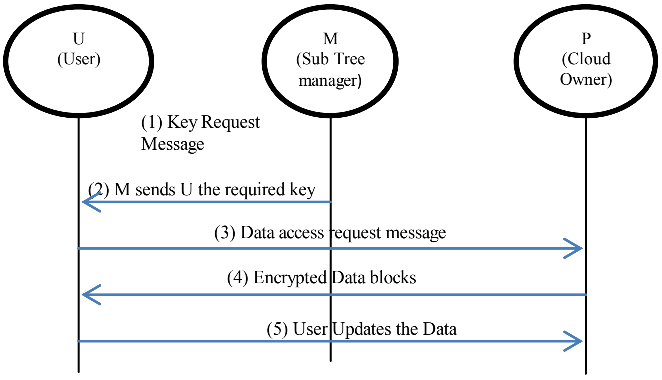

U
(User)
M
(Sub Tree
manager)
P
(Cloud
Owner)
(1) Key Request
Message
(2) M sends U the required key
(3) Data access request message
(4) Encrypted Data blocks
(5) User Updates the Data

Fig. 5. (b). Secure Key Distribution between Sub tree Manager and Cloud Owner.

Key derivation: This algorithm takes as input the master decryption key dij1 [8] and a one-way hash function H :{ 0, 1}* → Zp.It outputs the two child nodes of key dij1. By repeating this algorithm, the whole key derivation tree can be generated.

III. Conclusion

This paper discussed about the cloud data storage, users store their data and no longer possess the data locally. In the distributed cloud servers, the correctness and availability of the data files are being kept. One of the key issues is to efficiently detect any unauthorized data modification and exploitation. The Third Party Auditing permits to protect the time and computation resources with reduced online burden of users.

This work is to propose new algorithm to tackle all the difficulties of above mentioned algorithms. In the proposed method for encryption AES algorithm is used
And the raptor code is used instead of erasure code. Encode the input symbols using a traditional erasure correcting code, and then apply a proper LT-code to the new set of symbols in a way that the traditional code is capable of recovering all the input symbols even in face of a fixed fraction of erasures.

REFERENCES

[1] K.Ren, C.Wang, and Q.Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp.69-73, 2012.
[2] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Towards secure dependable storage in cloud computing," IEEE Services Computing, IEEE Transactions on vol.5, Issue.2, April-June 2012.
[3] D. Srinivasan, "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011.
[4] S. Kayalvizhi, Jagadeeswari, "Data dynamics for storage security and public auditability in cloud computing", February 10, 2012.
[5] T. Jaison Vimalraj, M.Manoj, "Enabling public verifiability and data dynamics for storage security in Cloud Computing", 2011.
[6] D.Shravani, Dr. S. Zahoor Ul Huq, "To Provide Security for Storage Services in Cloud Computing", IJCTT, vol4, issue 8, August 2013.
[7] Mooga Masthan, Dora Babu Sudarsa, "A secure cloud computing model based on multi cloud service providers," ijarcsse, volume.3, issue 5, May 2013.
[8] A. Miao Zhou, A. YiMu, A. WillySusilo, B. JunYan,A.C. LijuDong, "Privacy enhanced data outsourcing in the cloud",Journal of network and computer application,January 2012.
[9] http://arstechnica.com/business/2011/10/amazon-adds-server-side-encryption-to-s3-data-service/
[10] http://islab.csie.ncku.edu.tw/course/slide/ch_07.ppt.

[11] http://www.techopedia.com/definition/1763/advanced-encryption-standard-aes
[12] http://aws.amazon.com/about-aws/whats-new/2011/10/04/amazon-s3-announces-server-side-encryption-support/
[13] http://aws.typepad.com/aws/2011/10/new-amazon-s3-server-side-encryption.html.