ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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

V. Nithya[1], B. Anuradha[2]

II- M. Tech, Department of IT, SNS College of Engineering, Coimbatore, Tamil Nadu, India[1]

HOD, Department of IT, SNS College of Engineering, Coimbatore, Tamil Nadu, India[2]

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 a novel forward error correcting code algorithm as Raptor Code in which linear encode and decode can be done. This raptor code drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques.

Keywords: Data integrity, Raptor Codes, Security, Data dependability, Error localization, Data Dynamics**.**

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 centers 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Fig. 1 Cloud Computing

II. RELATED WORK

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 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. RAPTOR CODE

Most advanced forward error correction (FEC) code for data networks Raptor codes provide protection against packet loss by sending additional repair data used to reconstruct "erased" or "lost" data. Erasure codes provide data recovery by transforming a message into a longer message, agreeing the original message to be recovered from a subset of the expanded message. Raptor recovers missing data packets with only minimal amounts of additional repair data and without requiring retransmission from the sender an efficiently and effectively providing reliability in data networks.

Using a Raptor code [7], an application can send and receive encoded data, and the source properties of the solution avert, or greatly reduce the usage of feedback and retransmission protocols. This permits simpler, more scalable, and more effective solutions. Raptor codes may be systematic or non-systematic. In order to strike a good balance between error resilience and data dynamics, the algebraic property of the token computation and erasure-coded data is explored and demonstrate how to efficiently support dynamic operation on data blocks, which maintaining the same level of storage correctness assurance. In order to save the time, computation resources and related online burden of users, the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

extension of the proposed main scheme to support third-party auditing is provided, where users can safely delegate the integrity checking tasks to TPA and be worry-free to use the cloud storage services.

III. PROPOSED WORK

A. System Design

In the proposed model use the raptor code instead of erasure code. Encode the input symbols using a traditional erasure correcting code, and then apply an appropriate 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. To deal with the first issue, need to design the traditional code and the LT-code appropriately. Let Ω(x) be a linear code of block length and dimension, and let be a degree distribution. A Raptor code with parameters (k, C, Ω(x)) is an LT-code with distribution Ω(x) on symbols which are the coordinates of code words in C. The code C is called the pre-code of the Raptor code [7]. The input symbols of a Raptor code are the symbols used to construct the code word in C consisting of an intermediate symbols. LT-code are generated the output symbols from the n intermediate symbols. Typically, assume that is equipped with a systematic encoding, though this is not necessary. The definition of the encoding cost of a Raptor code differs slightly from that of a Fountain code. This is because the encoding cost of the pre-code has to be taken into account. The encoding cost of a Raptor code as E(c)/k+ Ω'(1), where E(c) is the number of arithmetic operations sufficient for generating a code word in from the input symbols. The encoding cost equals the per-symbol cost of generating k output symbols [7]. The decoding cost of a decoding algorithm for a Raptor code is the expected number of arithmetic operations sufficient to recover the k input symbols, divided by k. As with the Fountain codes, this cost counts the expected number of arithmetic operations per input symbol.

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+ε)K output symbols need to be ε for example, means that (1+ ε)K output symbols need to be collected to ensure successful decoding with high probability.
- Cost: The encoding and decoding process cost is less.

C. Result and Discussion

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 [8]. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

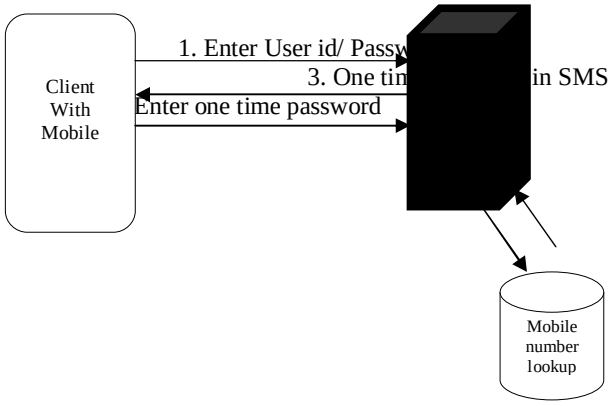

Fig. 2. One Time Pad Password Authentication.

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. 2 presents how a two factor authentication with one time pad mechanism is worked through mobile SMS.

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 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. For a user, who is authorized to access only the data block stored in the node and should not have access to its children, the manager only grants d2 to the user. 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 Mε{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

C1← (hk.g0k.g1k.g2k), C2 = M*hk (1)

Decryption: This algorithm takes as input the cipher text (c1,c2) and one of decryption keys d1 and d2, and outputs M * hk 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)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Key derivation: This algorithm takes as input the master decryption key dij1 [9] 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.

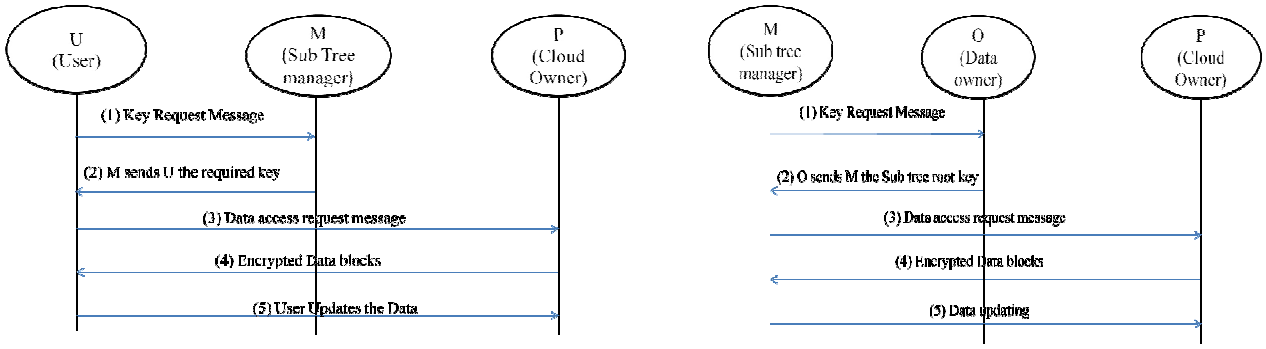

Fig. 3. Secure Key Distribution.

Implementation of Raptor code :To encode the input symbols using a traditional erasure correcting code, and then apply suitable 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. To deal with the first issue [6], need to design the traditional code and the LT-code appropriately. Let Ω(x) be a linear code of block length and dimension, and let be a degree distribution. A Raptor code with parameters (k, C, Ω(x)) is an LT-code with distribution Ω(x) on symbols which are the coordinates of code words in C. The code C is called the pre-code of the Raptor code. The input symbols of a Raptor code are the symbols used to construct the code word in C consisting of n intermediate symbols. LT-code are generated the output symbols from the n intermediate symbols. Typically, to assume that is equipped with a systematic encoding, though this is not necessary. The definition of the encoding cost of a Raptor code differs slightly from that of a Fountain code. This is because the encoding cost of the pre-code has to be taken into account. We define the encoding cost of a Raptor code as E(c)/k+ Ω', where E(c) is the number of arithmetic operations sufficient for generating a code word in from the input code symbols. The encoding cost equals the per-symbol cost of generating k output symbols.

The decoding cost of a decoding algorithm for a Raptor code is the expected number of arithmetic operations sufficient to recover the k input symbols, divided by k. As with the Fountain codes, this cost counts the expected number of arithmetic operations per input symbol.

IV. 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 the raptor code is used instead of erasure code. Encode the input symbols using a traditional erasure correcting code, and then apply an 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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. D. Srinivas, "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011.
3. S. Kayalvizhi ,Jagadeeswari, "Data dynamics for storage security and public auditability in cloud computing", February 10, 2012.
4. T. Jaison Vimalraj, M.Manoj, "Enabling public verifiability and data dynamics for storage security in Cloud Computing", 2011.
5. D.Shravani, Dr. S. Zahoor Ul Huq, "To Provide Security for Storage Services in Cloud Computing",IJCTT, vol4,issue 8,August 2013.
6. A.S. Anupriya, R. Anandhi, Dr. S. Karthik, "Secure cloud storage using Raptor code", ijser, vol.4, issue 8, August '13.
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. Bezawada Bruhadeshwar, Sandeep S. Kulkarni, "Balancing reocation and storage trade-offs in secure group communication," IEEE Transactions on dependable and secure computing,vol 8,no 1, January-February 2011