International Journal of Research

Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 05
March 2016

Enhanced Approach for Resolution to Data distribution for Confidentiality amid Data Owner and Service Provider

K. LALITHA
Associate Professor, Department of CSE
AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.
SK. IMRAN PASHA
Assistant Professor, Department of CSE
AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.
S.NITHA
M.Tech, Computer Science &Engineering
AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

Abstract: **Computing has been extensively used for data storage and computational purposes. When we talk about the cloud storage services, the data must be outsourced, so, there may be grave concerns about the authorization and trust management for the cloud service provider (CSP). These concerns are about confidentiality, integrity, security and access control. Cloud Service Provider (CSP) provides various types of services. Such as Storage-as-a-Service (SaaS) is a paid facility provided by CSP, where data owners can outsource their data in the cloud. This having some issue of ensuring the integrity and security of data storage in Cloud. We consider the work of allowing a Trusted Third Party (TTP), on behalf of the cloud client, to verify the integrity and security of the dynamic data stored in the cloud. The data owner securely outsources confidential data in cloud. It allows authorized users to access the owner's file. It maintains trust between data owner and cloud service provider.**

Index Terms: Trusted Auditor, Encryption, Access control, Dynamic environment and Outsources data storage

1. INTRODUCTION

Cloud Computing describes a new supplement & delivery model for IT services based on the Internet & it typically involves over- the-Internet provision of dynamically stable & often virtualized resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this Information age, several organizations posses huge amount of data which needs to be kept secured. These data includes personal information, health information and financial data. Local maintenance of such huge amount of data will be cost effective and problematic. Hence Cloud Service Provider offered Storage as a Service to alleviate the burden of huge local data storage and to reduce the cost by means of outsourcing data storage to the cloud.

Cloud computing is the long dreamed vision of computing as a utility, where data owners can store their data in the cloud storage to enjoy required high-quality applications and services from a shared pool of configurable computing resources. While data store in cloud server relieves the owners of the worrying of local data storage and maintenance, it also free their physical control of storage security and dependability, which usually has been expected by both organization and singular with high service level requirements. In the current period of digital world, various organizations produce a large amount of sensitive data including personal/confidential information, electronic health records, and economic/financial data. The local management of such large amount of data is challenging and expensive due to the requirements of large storage capacity and qualified staff. Therefore, Storage-as-a-Service offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. We consider a scenario in which a large, confidential file is to be stored securely over cloud networks. These networks are not trustworthy in the sense that an attacker may gain access to some of them, but not to all.

In some practical applications data confidentiality is not only a security concern but also a juristic issue. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote cloud server. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites.

In order to achieve the assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient techniques that enable required data correctness verification on behalf of cloud users have to be designed. Security audit is an important solution enabling trace back and analysis of any activities including data accesses, security breaches, service activities, and so on. To ensure there is no attack to compromise the security of verification protocol or cryptosystem by using dynamic data operations. We provide the security to owner's data by using RC5 algorithm.

2. RELATED WORK

Existing work related to our proposed work can be found in the areas of integrity verification of remotely stored data and file encryption schemes in distributed systems and access control mechanisms over outsourced data. A model for provable data possession (PDP) by Ateniese et al. that allows a client that has stored data at an un-trusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server. It reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The response protocol transmits a small, constant amount of data, which reduces network traffic. Thus, the PDP model for remote data checking supports large data sets in Widely-distributed storage system.

2.1 System component and Assumption:

The Mutual trust between the data owner and the CSP is another issue and that is addressed in this scheme. A mechanism is introduced to determine the dishonest party, from any side is detected and the responsible party is identified. Access control is also provided by the model which allows the owner to grant access or to revoke access rights to the outsourced data.

The cloud storage model consider in this work consists of four components as illustrated in Fig. 1: (i) A data owner that can be an any organization/Company generating sensitive data to be stored in cloud storage and make available for controlled external use, (ii) A Cloud service provider who manage cloud server and provides storage space on its service to store the owner's data and made them available for authorized users, (iii) authorized user's: group of owner's clients who have the authority to access the cloud storage data; and (iv) a Trusted Third Party (TTP), an unit who is trusted by

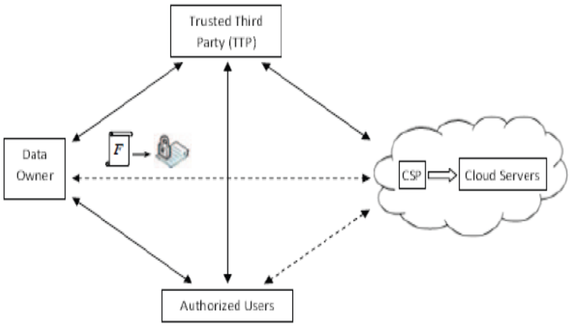


Fig. 1: Component and Cloud Storage

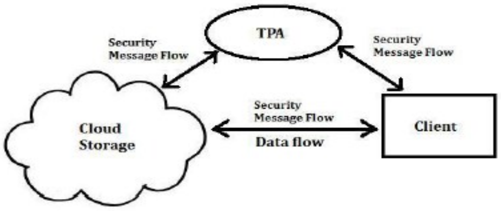
data owner, and has capabilities to detect/specify unauthorized parties.

2.2 Security Requirement:

Confidentiality: Protect the cloud data from Cloud Service Provider (CSP), unauthorized user and Trusted Third Party (TTP) which have no permission.
Integrity: The cloud server data should remain undamaged i.e. the outsourced data.
Newness: The latest copy of outsourced data should receive.
Access Control: The outsource data access permission are granted to only authorized users.
Defense: The Cloud Service Provider has to be protected from fake allegation that might be claimed by lying owner / user.

3. IMPLEMENTATION

In these paper we propose four important component's/module's: first O-Module (Owner module), second C-Module (CSP module), third A-Module (Authorized user module), and forth one is T-Module (TTP module).



O-Module that runs on the owner side is a documentation which is used by the owner to carry out the owner function in the system and file training phase. Additionally, this documentation is used by the owner at some stage in the dynamic operations on the cloud data.

Commonly, traditional access control techniques assume the existence of the data owner and the storage servers in the same trust domain. This assumption, however, no longer holds when the data is outsourced to a remote CSP, which takes the full charge of the outsourced data management, and resides outside the trust domain of the data owner. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. This general solution has been widely incorporated into existing schemeswhich aim at providing data storage security on untrusted remote servers. Another class of solutions utilizes attribute-based encryption (ABE) to achieve fine-grained access control. ABE is a public key cryptosystem for one-to-many communications that enables fine-grained sharing of encrypted data.

There is also solution provided by introducing trusted third party auditor (TTPA), into the cloud system. That is on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The TTPA replaces the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be commercially important Cloud Computing. The data operations such as block modification, insertion and deletion, is also a significant. The public verifiability and dynamic data operations are provided in this model of TTPA The proof of retrievability model is modified by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. The Extensive security and performance is proposed in TPA model and provably secure.

RC5 Algorithm:

RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choices of parameters were a block size of 64 bits, a 128-bit key and 12 rounds. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a crypto-graphic organelles. RC5 algorithm also consists of a number of eXclusive OR (XOR)'s and the modular's addition. The general arrangement of the RC5 algorithm is a Feistel as a network. The process of encryption and decryption repetitive can be specified in a few numbers of codes. The schedule of key, however, is more complicated, expanding the key using an necessary one path function with the binary growth of both e and the excellent ratio as sources of "nothing up along my sleeves numbers". The inviting ease of the RC5 algorithm together with the experience of the data contingent rotations has made RC5 an attractive goal of study for crypt-analysts. The RC5 is essentially denoted as RC5 - w/r/b where w = word size in bits, r = number of rounds, b = number of 8-bit byte in the key.

In this part we brief the RC5 algorithm, which have three components: The RC5 key expansion algorithm for a RC5 encryption algorithm and RC5 decryption algorithm, we summaries the encryption & decryption algorithms first.

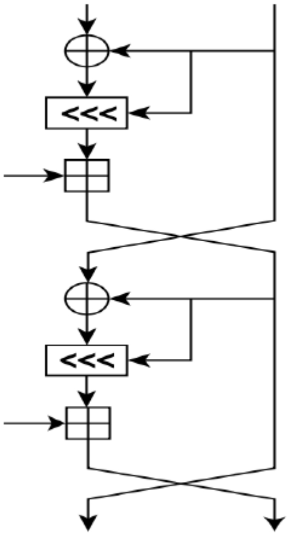


Fig. 2: one round (two half-rounds) of the RC5 block

Recall the plaintext that input to RC5 algorithm consists of two w - bit words, which is denoted by A and B. Recall also that the RC5 algorithm uses an expanded key table S[0…t-1], consisting of t = 2(r + 1) w - bit words. The RC5 key expansion algorithm initialize S from the secret key parameter K which is given by users. (Note that the S table in RC5 encryption algorithm is not an "S - box" such as is used by DES algorithm; RC5 uses the entries in S sequentially, at a same time.)

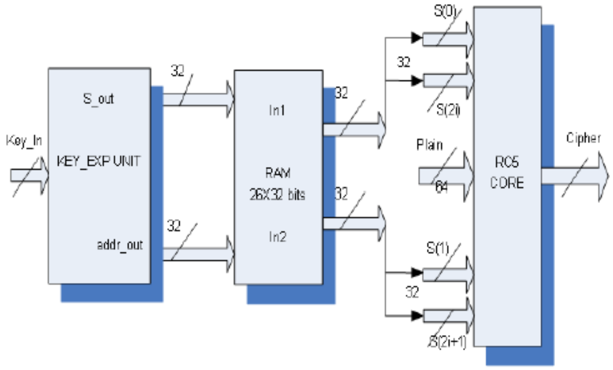


Fig. 3: Architecture of the RC5

We take standard little-endian gathering for packing bytes into I/O (input/output) blocks: the first byte hold the low - order bit positions of register A, and so on, so that the fourth byte hold the high - order bit positions in A, the fifth byte hold the low - order bit positions in B, and the eighth (last) byte hold the high - order bit positions in B.

Encryption:

We assume that the input block is given in two w - bit registers A and B. We also assume that key - expansion has already been performed, so that the array S [0…t-1] has been computed. Here is the encryption algorithm in pseudo - code:

```
A = A + S [0];
B = B + S [1];
for i = 1 to r do
A = ((A B) <<< B) + S[ 2 * i ];
B = ((B A) <<< A) + S[ 2 * i + 1];
```

The output is in the registers A and B.

We note the outstanding simplicity of this 5 - line algorithm. We also note that each RC5 algorithm round updates both registers A and B, where as a "round" in DES algorithm updates only half of its registers. An RC5 algorithm "half - round" (one of the assignment statements updating A or B in the body of the loop above) is thus perhaps more analogous to a DES round.

Decryption:

The decryption algorithm routine is easily derived from the encryption algorithm routine.

```
for i = r downto 1 do
B = (( B – S[2 * i + 1]) >>> A) A;
A = (( A – S[2 * i ]) >>> B) B;
B = B – S[1];
A = A – S[0];
```

Key Expansion:

The key-expansion routine expands the user's secret key K to fill the expanded key array S, so that S resembles an array of t = 2(r + 1) random binary words determined by K. The key expansion algorithm uses two "magic constants," and consists of three simple algorithmic parts and provide following features.

□ It allows the data owner to outsource confidential/sensitive data to a cloud server data, and perform full block level dynamic operations on the cloud data, i.e., block modification, insertion, deletion, and append.

□ It ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the cloud server data.

□ It enables indirect mutual trust between the owner and the CSP.

□ It allows the data owner to grant or revoke access to the cloud server data. We discuss the security problem of the proposed scheme. Moreover, we justify its performance through speculative analysis and a prototype implementation on Amazon cloud platform to assess storage, communication, and computation expenses.

4. CONCLUSION

The storage model used in this work can be adopted by many practical applications. For example, e-Health applications can be envisioned by this model, where the patients' database that contains large and sensitive information can be stored on cloud servers.There is outsourcing of data over the cloud service provider. Thus there are serious concerns about the cloud storage systems, so there are various schemes have been introduced. These models are about trust and security for the cloud storage systems. In this scheme, the owner is capable of archiving and accessing the data stored by the CSP and updating and scaling this data on the remote servers. This scheme enables newness of data. The trusted third party has been introduced in this model which determines whether the storage is honest or not. It detects the party. The data owner can not only archiving and accessing the data stored by the Cloud Service Provider, but also manipulate and scaling this data on the cloud servers. The offered scheme enables the right/valid users to ensure that they are receiving the recent copy of the outsourced data. Additionally, in case of dispute about data integrity/originality, a TTP is able to determine the lying party.

REFERENCES:

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[2] Sehgal NK, et al.: Information Security and Cloud Computing, Iete Technical Review, Vol 28, Issue 4, Jul-Aug 2011..

[3] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: multiple replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.

[5] Ayad Barsoum and Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on parallel and distributed systems, 2013.

[6] Cong Wang and Kui Ren, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, August 2010.

[7] Paulo F. Oliveira, "Coding for Trusted Storage in Untrusted Networks," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, December 2012.

[8] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lo, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, Vol. 5, No. 2, June 2012.

[9] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions On Services Computing, Vol. 6, No. 2, June 2013.

[10] Ron Rivest, "From Wikipedia, the free encyclopedia", http://en.wikipedia.org/wiki/RC5, March 1997.

Authors

K. LALITHA Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad. Currently working as an Associate Professor at AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

SK. IMRAN PASHA Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad. Currently working as an Assistant Professor at AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

S.NITHA pursing M.Tech in Computer Science Engineering from AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.