Analysis of Efficient Algorithms in Cloud Computing for Cloud Data Storage and Security Management

Nisha Rani*

Computer Science

Abstract – A further computing paradigm is cloud computing in data innovation. Cloud computing is characterized by the National Institute of Standards and Technology (NIST) as taking into account the ubiquitous, helpful, on-demand organize access to a mutual pool of configurable computer assets. In this study we focused on data storage system model in cloud computing paradigm and data security issues are listed on cloud system as well as challenges.

Keywords: Cloud Computing, Data Storage, Cloud Computing Paradigm, Security Management

- X -

INTRODUCTION

In the cloud computing paradigm, cloud storage becomes an expanding fascination, allowing customers to pay more only as costs arise to store their information and access it anywhere and at whatever point they need to use any gadget. Moving data into the cloud provides users with great convenience as they don't have to worry about the large investment in both maintaining and managing hardware infrastructure. Known examples of cloud data storage are Amazon's Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) and apple icloud. However, the users lose control over the data once data goes into the cloud. This lack of control brings forth new formidable and challenging issues related to the confidentiality and integrity of cloud-based data.

The rise in cloud computing use has reduced activity costs, versatility, and simpler access has prepared for wider use of distributed storage management. Cloud storage administrations cause customers to anchor their neighborhood risk information just as convenience is enhanced. In addition, a similar idea helps to impart information to different customers and work on the same venture all the time. This prompts a noteworthy issue of the same information being transferred to their capacity servers among Cloud Service Provider (CSP). Clients number store their valuable data in the cloud. This results in loss of memory capacity and making customer access slower. Hence, in order to make distributed storage increasingly productive deduplication of information was proposed by Zheng Yan, et al Proposed deduplication dependent on possession testing and intermediate re-encoding. This framework used an additional external framework that guarantees control of information proprietors and makes cloud specialists co-op as intermediaries between the two. It included assumptions that the outside party would remain free from any arrangement with some other customer or CSP itself.(1) Storage as a Service (STaaS) Cloud has, as of late, taken on ubiquity among both private clients and organizations (2). STaaS is a Cloud action plan in which a specialist organization provides space in its stockpiling framework for individuals or organizations. New information models are being developed to deliver capacity dependent on information objects with rich, extensible metadata and expanding approach techniques, locating cloud-based capacity foundations as the cutting-edge response to expanding and information dependence. The data stored in the cloud may be enterprise sensitive.

The problem is that the provider or other unauthorized persons will likely exploit those data. Most cloud storage users currently protect their data with SLAs contracts, and are based on the provider's trust and reputation. This weakness has motivated us to think about solutions that enable users to secure their data to prevent malicious use. Regardless of the qualities that speak to cloud computing for the most part and cloud storage exceptionally; there are different research difficulties, both from an industry and an institution's perspective, such frameworks need to be delivered in order to conquer confines identified with issues such as versatility, interoperability, storage access, security, cost, productivity vitality.

Security (particularly associated with users ' personal sphere, compliance with legislation, and trust issues) is a major impediment to its spread. There are various opinions on cloud computing security that deal with the positive and negative aspects of it(3)

SECURITY

Cloud computing security involves concepts such as network security, deployed equipment and control strategies for protecting cloud computing related data, applications and infrastructure. An important aspect of cloud is the notion of interconnecting with different materials which makes the securing of these environments difficult and necessary. Security issues in a cloud platform can lead to economic loss, but also a bad reputation if the platform is geared towards a wide audience and is the cause behind the massive adoption of this new solution. Customer data stored in the cloud is vitally important information.

It is therefore unacceptable for such data to be infringed by an unauthorized third Party. In Cloud, there are two ways to attack the data. One is attacking outsiders and the other is attacking insiders. Insider as an administrator may have the option of hacking user data. It's really hard to identify an insider attack. The users should therefore be very careful when storing their data in cloud storage. Hence the need to think about methods that impede data use even if the third party accesses the data; they should not get the actual data. So, before it is transmitted to cloud storage, all data must be encrypted. (4) Security allows information to be kept confidential, complete, authentic and accessible. The development of technologies and their standardization makes a set of algorithms and protocols available to respond to these problems (5, 6).

CLOUD SYSTEM ARCHITECTURE

Cloud storage assets as a customer-accessible help over the Internet, cloud computing as a support framework (LAAS foundation as a help) is a kind of important structure, and it's deep in our lives. Cloud stockpiling has numerous exceptional conventional stockpiling benefits, such as the multi-faceted nature of the customer protecting executives ' base equipment, organizing on-demand assets whenever and whenever possible. Some well-known IT companies have played an important role in recent years and have started providing cloud storage services such as their cloud computing, such as Amazon J Simple Storage 100 Service (S3), Google Cloud Storage, and Rackspace Cloud Files. Additionally appearing on cloud storage framework administrations, e.g. the upper application administrations, e.g. online record storage and strengthening administrations from EMC organization, Mozy, etc. While it has many advantages and has been sought-after by many IT companies, however, cloud storage has not been widely used, one of the major reasons is that data security problems.

The key data security technology in cloud storage is a broad concept which contains many aspects, so the main content of this paper needs to be explained. The cloud storage data security study has a lot of research work, cloud storage in access control, and so on. This paper reads the quest for a figure message; the primary concern is the information's accessibility and reliability. (7)

Our study focuses on three basic issues:

1) how users are kept informed quickly and in a timely manner of their data stored in the cloud;

2) how to restore it if the data is not in good condition;

3) how to implement key technology to solve problems in the actual cloud storage environment.

Typically, the information is not placed entirely in a hub in the cloud storage condition, yet is divided into different cuts and then placed on various capacity hubs at irregular intervals. This strategy is like paging the board's memory, can successfully decrease the record size of non-bringing hub storage pieces, upgrade additional room usage, and can forestall hub assault making all hole customer information. In any case, the deadly blemish of this strategy is that a hub is harmed, and because of the loss of the fracture, countless documents cannot be finished. The cutting of information repetition is expected to endure a particular extent of the misfortune, so regardless of whether a couple of hubs breakdown cut in the Qing, the document can in any case be attained by the included capacity hub.

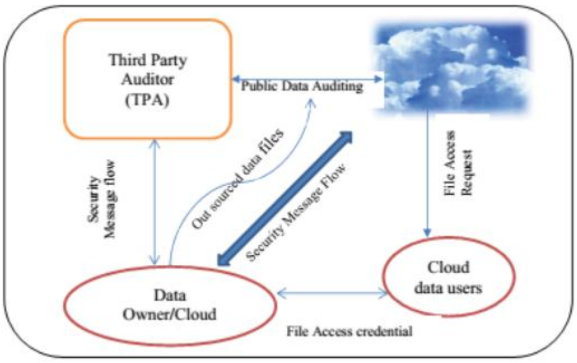


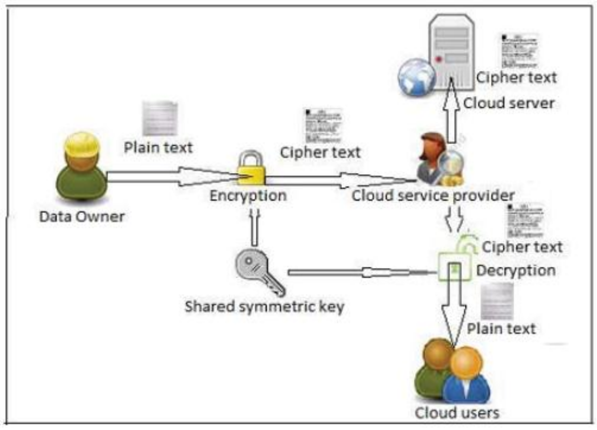
Figure 1.1: Cloud Data Storage System Model

A workload distribution scheme like Online / Offline Provable Data Possession data auditing on cloud server has been proposed in Yujue Wang et al.. In his method the light weights file processing computations are assigned to the offline mode and heavy weight computation to the online mode. The main drawback of this method is the segregation of light and heavy workload has a challenging task.(8) Cong Wang et al., proposed a ranked keyword search for secure data access over the outsourced cloud information. In this method, the data owner sends the data file to the cloud server along with the list of keywords in the data. The cloud server can derive the outsourced data using shared keywords and its frequency. So that, there is no privacy of the outsourced data from the untrusted cloud server. Besides, this the cloud service provider can also delete the rarely accessed data from the cloud storage for his storage space benefits.(9)

PROPOSED DATA AUDITING SCHEMES

Data Encryption using Key Rotation

Some of the data protection techniques include data protection in the cloud, authentication and integrity, access control, encryption, integrity checking, and data masking. In cloud computing, cryptography is one of the efficient methods of data security. Which includes designing and implementing an effective algorithm for encryption and decryption. In symmetric cryptography, data is encrypted into cypher text using a secret key before outsourcing to the cloud server and later decrypted with the same shared secret key.



Key management to data encryption and decryption is the most critical part for implementing any of this method. The common way of protecting data in motion is by using authentication encryption, which securely passes data to or from the cloud server. Data owners in cloud computing are increasingly outsourcing their sensitive data in encrypted form from local system to public cloud for greater flexibility and economic savings (10, 11).

Algorithms

The encryption algorithm will disguise highest factor information by applying series of rotations to each block character, and the key will be rotated for each character. This ensures that the same key is not used to encrypt each character and is therefore called this algorithm as the key engine encryption algorithm.

The decryption process in algorithm 2 suggests that first CA shifter is performed, then the key selector component is used to select two keys and added before CA is inverted. As CA already contains added value and CA complement now yields original encoded value. To get its original character the Encoding Map Em is searched. The Algorithm has the same complexity as the algorithm for encryption.

DATA AUDIT USING PROTOCOL

System model

It consists of five components such as; key generator, cloud servers, verifier, cloud users, and combiner. Key generator: It is an entity, which receives the identity of the user(ID) and generates the secret key(sk_id) for the user(ID) using a computational Diffie-Hellman (CDH) method.

Alg. 3 Data Access Procedure Algorithm steps :

1. An authorized user sends a request to both the CSP and TTP auditor.

2. CSP sends the encrypted file and BST to the requested user.

3. TTP sends the FHttp, T Http and key to the user.

4. user computes the T Huser using T Hcsp and FHuser using data blocks. Then compared with stored T Http and FHttp respectively for integrity check.

5. If both BST and file computed hash values are matches, then user decrypt the file using shared secret key

Basic Auditing Scheme

The basic data integrity verification scheme consists of three stages such as; key generation, meta data generation and data audit.

Data verification

After the encrypted file and meta-data of the file outsourced to a cloud server, the TPA can check the integrity of the data blocks periodically for the favor of data owner. The data verification is a sequence of request and response message between CSP and TPA. For every request from TPA, the CSP generates a response as a proof and sent to TPA. The data verification consists of a challenge message generation, proof generation and proof verification phases.

Batch auditing

In the proposed data auditing method, the TPA is not only audit the single data owner single file, but also support multiple user and multiple file data auditing tasks. Hence, batch auditing is also introduced in the proposed design. The batch auditing tasks are considered in two ways; single data owner with multiple files and multiple data owners with multiple files. Let consider a data owner DOi having fij list files, where i = 1 to s, j is the i th data owner files. In public auditing, the data owners delegate the batch auditing task to TPA.

RESULTS AND ANALYSIS

Remote Data Audit using Protocol (RDAP)

Communication Cost:

The design of the proposed method consists of the initial phase of file setting up and data auditing. The audit phase is a sequence of communication of requests and responses between Data owner, TPA and CSP. For each data review, TPA prepares a test message and sends it to the CSP. The message of challenge contains the c number of identifiers of data blocks, so the cost of communication between TPA and CSP is O(c).

Computation Cost:

We are considered the tag generation time, tag verification time and data verification time with different file sizes, data block sizes and audit batch sizes for measuring the computation cost of the proposed remote data auditing method using identity-based and linear authentication-based method.

RDADS Simulation

Computation Cost We use the sampling auditing method to verify the outsourced data in the cloud, due to the large data file. In the following section, the computation costs of the TPA and CSP for auditing data blocks on a single server and multiple data owners are given. The performance analysis of the internal computation cost RDASDS and RDAP methods is analyzed using the following parameters: Signature generation cost, File setup and upload time, Data block verification time, Modified data block detection, CSP vs TPA computation time, RDAP vs RDADS signature, and data verification.

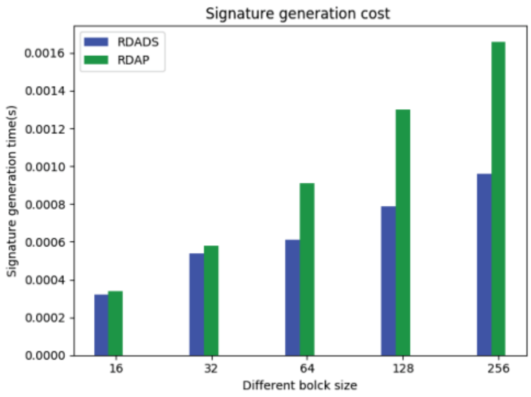
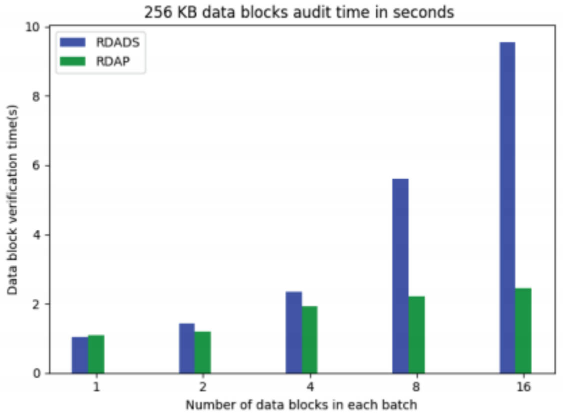


Figure 6.3: Signature generation cost for different blocks

Data Audit Time:

As shown in Figure 6.5, the computational cost comparison between RDADS and RDAP method for auditing different number of 256 KB data blocks challenging task. The X-axis represents the different number of data blocks in each batch in Figure 6.5, and the Y-axis represents the cost of data verification between TPA and CSP. The result shows that the RDADS method costs more than the RDAP method for the larger batch size. During the data verification phase these changes are involved in RDADS due to the expensive operations of elliptic curve points. But the RDADS method is better from a security point of view than the RDAP method.



Computation Cost Comparison between CSP and TPA:

Comparison of overhead calculations between TPA and CSP for 50 KB of audit data blocks.

TPA takes the same computation cost as 50 KB blocks, compared to 256 KB of data blocks. But in both cases the cost of CSP computation varies depending on the batch size.

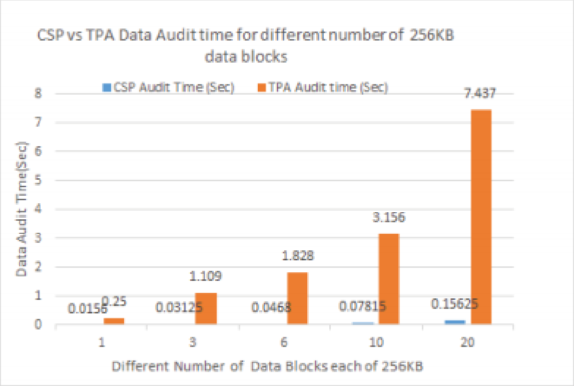


Figure 6.7: CSP and TPA 256KB Data Blocks Audit Time(Sec)

CONCLUSION

It is concluded that data confidentiality and remote data integrity verification are used to tackle cloud data privacy and security issues. We've provided a protocol and digital signature based on approaches to cryptography to address cloud data security problems. Finally, we believe that security challenges to cloud data storage are not limited, and it is also an important research area for secure data sharing in cloud computing.

REFERENCES

1. Zheng yan, Wenxiu Ding, Xi Xun Yu, Haiqi Zhu, ET ALand Robert H. Deng. Deduplication on Encrypted Big Data in Cloud. IEEE Computer Society.

2. [1] KOLODNER, Elliot K., TAL, Sivan, KYRIAZIS, Dimosthenis, et al. A cloud environment for data-intensive storage services. In : Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 357-366.

3. P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, « Cloud Computing Security Issues in Infrastructure as a Service », Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no 1, 2012.

4. L. Arockiam, S. Monikandan (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm » International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

5. Taher ElGamal (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, pp. 469-472,.

6. Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

7. Huang Ruwei, Gui Lin, Yu Si, Zhuang Wei. Cloud environment in support of the privacy protection can be calculated encryption method [J]. Journal of the computer. 2011 (12).

8. B. Q. W. S. R. H. D. Yujue Wang, Qianhong Wu and J. Hu, "Identity-based data outsourcing with comprehensive auditing in clouds," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 940–952, APRIL 2017.

9. C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, 2012.

10. J R Winkler, "Securing the cloud: Cloud computing security techniques and tactics," Elsvier Inc.,USA, 2011.

11. Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud securityand privacy," Published by O Reilly Media, Inc.,, 2009.

Corresponding Author

Nisha Rani*

Computer Science