ISSN:0975-9646

A Result Analysis on Privacy-Preserving Public Auditing System of Data Storage Security in Cloud Computing through Trusted TPA

Nupoor M. Yawale, Prof. V. B. Gadicha

[#]*M.E. Second year CSE*
P R Patil COET, Amravati. INDIA.

[*]*HOD, P R Patil COET*
Amravati. INDIA.

***Abstract*— Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Many users place their data in the cloud, so correctness of data and security is a prime concern.**

Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interconnecting the large-scalecomputing resources to effectively integrate, and to computing resources as a service to users.

To ensure the correctness of data, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

In this research paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audit efficiently with RC5 Encryption Algorithm. Resulted encrypted method is secure and easy to use.

***Keywords*— Cloud computing, Encryption, privacy-preserving, public auditability, RC5 Algorithm, Third Party Auditor (TPA).**

I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1].

Cloud computing is foreseen to be the upcoming architecture to be employed in industries, owing to its vast merits in information technology history. Need for self-services, universal network processing of a network location autonomous resources availability, spontaneous resources flexibility, pricing is determined on the level of usage also on the risk of the transfer [2]. As a disarray invention with foreseen implication, cloud computing is mending way it uses business with IT. The basic point of view pattern is changing the way it is being focused over the cloud. In the views of users i.e. combining individuals and IT industries, storing the data remotely on cloud bring more benefits. Manual storage is completely lessened, we can access it universally with ubiquitous geographical location, the expenditure on hardware, software and personal maintenance is brought down [3]. In addition to this advantage it brings forth exclusive and challenging security threats towards user's outsourced data.

As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [4].

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted [5]. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users [3][6].

Moreover, the overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data. For example, it is desirable that users do not need to worry about the need to verify the integrity of the data before or after the data retrieval. Besides, there may be more than one user accesses the same cloud storage, say in an enterprise setting. For easier management, it is desirable that the cloud server only entertains verification request from a single designated party.

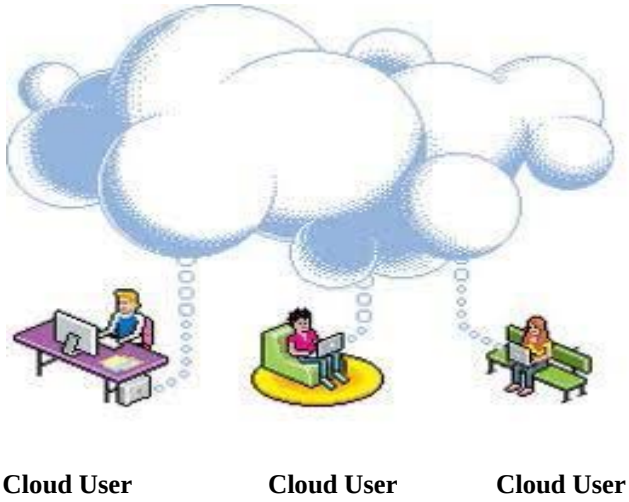

Fig. 1 Cloud Architecture

A. *Objectives*

- To provide data storage security in Cloud Computing using Third Party Auditor (TPA) Scheme.
- To design a scheme which will provide a monitoring system for preserving the confidentiality of the data.
- To support data integrity & validation through challenge and challenge verification.
- To established security for user's outsourced data without learning knowledge of data contents.

II. EXISTING SYSTEM

Cloud improves due to centralization of data, increased security focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 2 the cloud user (CU), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by the cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources; the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. To save the computation resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA.

We consider the existence of a semi-trusted CS as [7] does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. However, it harms the user if the TPA could learn the outsourced data after the audit. To authorize the CS to respond to the audit delegated to TPA's, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are authenticated against such a certificate. These authentication handshakes are omitted in the following presentation.

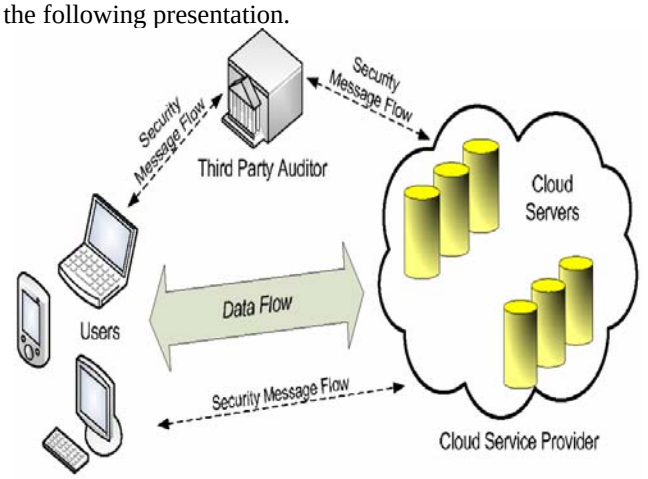

Fig. 2 The architecture of cloud data storage service

A. *Limitation of Existing System*

- User's files are not encrypted on some open source cloud storage systems. So, privacy is not preserve.
- The storage service provider can easily access the user's files. This brings a big concern about user's privacy.
- The user has no supreme control over the software applications including secret data. User has to depend on the provider's action, maintenance and admin it.

III. BASIC IDEA OF PROPOSED SYSTEM

In current research paper, the TPA will be able to properly monitor confidentiality and flexibility to the data and uniquely integrate it with encryption technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure.

The use of RC5 algorithm for encryption, cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key cannot be restored.

Only the TPA knows the key, the CSP do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

IV. SYSTEM IMPLEMENTATION METHODOLOGY

Cloud computing is nowadays evolving as a revolution. In cloud computing, cloud security is one of the most challenging tasks. Cloud computing entrusts services with users data, software and computation on a published application programming interface over a network. The cloud provides a platform for many types of services.

Cloud application providers strive to give the same or better service and performance than if the software programs were installed. When we talk about cloud Security, maintaining data integrity is one of the most important and difficult task. When we talk about cloud users, they are using cloud services provided by the cloud provider [2]. Again, in case of maintaining the integrity of the data, we cannot trust the service provider to handle the data, as he himself can modify the original data and the integrity may be lost. So, in this case, we take the help of a trusted third party auditor to check for the integrity of our data. This third party auditor takes care of our data and makes sure that the data integrity is maintained.

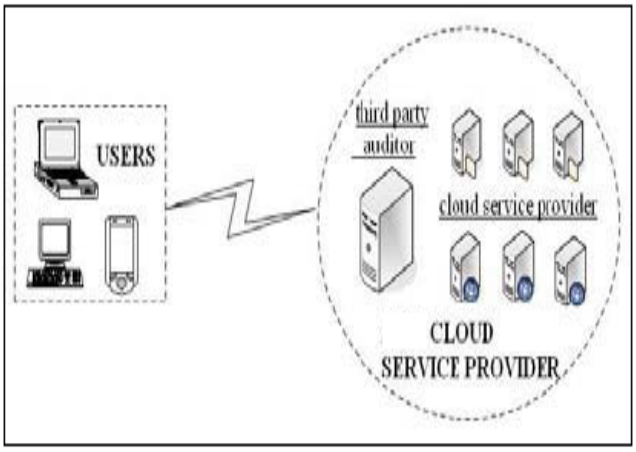

Fig. 3 TPA with Cloud Service Provider

To enable privacy-preserving public auditing for cloud data storage under the mentioned model, our protocol design should achieve the following security and performance guarantees. Public auditability to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. Privacy-preserving to ensure that the TPA cannot derive users data content from the information collected during the auditing process.

In proposed method we use RC5 algorithm for encryption and decryption. In our protocol there are three main participants. As discussed above (i) Third Party Auditor (TPA) (ii) User (iii) Cloud Service Provider. We consider a cloud data storage service involving three different entities. The cloud user or owner (CU), who has large amount of data files to be, stored in the cloud; the Third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the TPA for cloud data storage and maintenance. To save the computation resource as well as the online burden, cloud users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA. Cloud service provider (CSP), provides data storage service and has significant storage space and computation resources.
We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CSP or the users during the auditing process.

One of the best ways to ensure confidential data is protected in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for data storage, but few offer support for data at rest. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. To protect a user‘s confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only user can confidently utilize cloud providers knowing that their confidential data is protected by encryption.

V. MODULES

In current research paper, the TPA will be able to properly monitor confidentiality and integrity of the data to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. The use of RC5 algorithm for encryption, cloud computing can be applied to the data transmission security. Proposed system mainly consists of four modules which are listed below:

- Login Module
- Third Party Auditor
- Cryptography
- Privacy-preserving

A. Login Module

In this module, there is multiple login

- User Login
- CSP login
- TPA login

The role of User, CSP and TPA are as follows-

Initially user can register himself or herself with specific information. Then user can simply store data, file or application on cloud and received original decrypted data from cloud.

TPA should encrypt and decrypt all users’ data and save encrypted data on cloud. Also data integrity validation is done through challenge and challenge verification. TPA has privileges to see user’s original data as well as encrypted data.

CSP provide space for storing data on cloud and response to challenge. But CSP doesn’t have any privilege to see the original content of users file or data. So that privacy is preserved.

B. Third Party Auditor

In this module, Auditor (TPA) views all List of Files Uploaded by User. Auditor directly views all user data without key. TPA has privileges to encrypt the user's data and save it on cloud. Also auditor can view data which is uploaded by various users. TPA can encrypt data and send it to Cloud service provider (CSP) for storage and auditor can view encrypted data of every user.

C. Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

In our scheme, we had used RC5 Algorithm to perform encryption and decryption on user's data. Due to encryption privacy is preserved as no one can see your data.

D. Privacy-Preserving

To ensure that the TPA cannot derive users' data content from the information collected during the auditing process. As our auditor is trusted Third Party Auditor, privacy is preserved. There is privilege for user to see only the files uploaded by that user only and not by other user. Privacy is preserved by both user and cloud service provider (CSP) as they don't have right to view the content of file.

VI. ADVANTAGES

- The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.
- User can store any file or application on cloud and received the original decrypted data from cloud.
- TPA can save encrypted data on cloud and perform data integrity validation through challenge & challenge verification.
- CSP can provide simply the space for storing the file and it doesn't have privilege to see the content of file as it is stored in encrypted form.

VII. APPLICATIONS

- Clients would be able to access their applications and data from anywhere at any time and data should be fully secured as it is stored in encrypted form.
- This system can be deployed in school for students. The admin will store electronic teaching materials on cloud servers. This will not only make it possible for students to use online teaching materials during class but they will also be able to access these materials at home, using them to prepare for and review school lesson.
- This system can be implementing in Banking Sector for storing confidential data on cloud.
- The system can be used in various corporate applications which are seeking for the confidentiality & Integrity of the data in cloud environment.

VIII. RESULT ANALYSIS

In the field of compiler implementation in computer science, constructed product result analysis (or CPR analysis) is a static analysis that determines which functions in a given program can return multiple results in an efficient manner.

We now assess the performance of the proposed privacy-preserving public auditing schemes to show that they are indeed lightweight. We will focus on the execution time of the privacy-preserving system. The experiment is conducted using three algorithm i.e. RC5 algorithm, RSA algorithm and DES algorithm.

TABLE 1
EXECUTION TIME FOR FILES WITH RC5, RSA AND DES ALGORITHM

File name	File Size (KB)	Execution Time with RC5 (ms)	Execution Time with RSA (ms)	Execution Time with DES (ms)
supervisisor_list2012.pdf	337	109.375	178.5	340.5
hi.doc	10	125	200.8125	364.25
nupoor.txt	4	94.3	120.4	150.54
chrysanthemum.jpeg	860	234.375	320	532.625

Table 1 Shows Execution Time for files with RC5, RSA and DES Algorithm. The execution time for RC5 is very less as compare to DES and RSA Algorithm. From this we can say that RC5 algorithm is efficient than other two algorithm.

The following Figure 4 shows graph representation of above Table. It can display the comparison of RC5, RSA and DES algorithm with respect to Execution time.

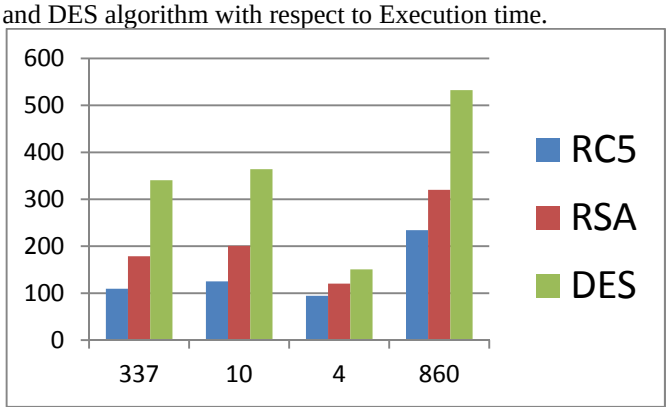

Fig. 4 Comparison of RC5, RSA and DES Algorithm w.r.t Execution time

This scheme provides a monitoring system for preserving the confidentiality of the data. Confidentiality is preserve through Third Party Auditor (TPA). Also it can support data integrity & validation through challenge and challenge verification.

IX. CONCLUSION AND FUTURE SCOPE

Cloud Computing is an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. System uses encryption/decryption keys of user‘s data and stores it on remote server. Each storage server has an encrypted file system which encrypts the client‘s data and store. The system ensures that the client‘s data is stored only on trusted storage servers and it cannot be accessed by administrators or intruders. TPA can perform auditing tasks. Resulted encrypted method is secure and easy to use. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. This research paper provides cloud data security using third party auditor.

We can implement this model in various cloud computing platforms to get the more efficient way of cloud computing such as SaaS, AaaS etc. we will also work on authentication of users password. In future, we can work for session key implementation for displaying the number of list uploaded by user and also display the encrypted image & multimedia messages.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing” Referenced on June. 3rd 2009 [cited 30 April, 2010]; Available from: http:// www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.[Online, Access: 15 Oct 2013]

[2] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage services honest,” in *Proc. Of HotOS’07*. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in *Proc. of ESORICS’09, volume 5789 of LNCS*. Springer-Verlag, Sep. 2009, pp. 355–370.

[4] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep, 2009.

[5] A. Juels and J. Burton S. Kaliski, “Pors: Proofs of retrievability for large files,” in *Proc. of CCS’07*, Alexandria, VA, October 2007, pp. 584–597.

[6] "Jeff Bezos' Risky Bet". *Business Week*, November 12, 2006.

[7] B Rochwerger, J Caceres, RS Montero, D Breitgand, E Elmroth, A Galis, E Levy, IM Llorente, K Nagin, Y Wolfsthal, E Elmroth, J Caceres, M Ben-Yehuda, W Emmerich, F Galan. "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4. (2009)

[8] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” *J. Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[9] A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, “Practical short signature batch verification,” in *Proceedings of CT-RSA, volume 5473 of LNCS*. Springer-Verlag, 2009, pp. 309–324.

[10] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in *Proc. Of SecureComm’08*, 2008, pp. 1–10.

[11] C.Wang, Q.Wang, K. Ren, and W. Lou, “Ensuring data storage security in cloud computing,” in *Proc. of IWQoS’09*, July 2009,pp. 1–9.

[12] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in *Proc. of CCS’09*, 2009, pp. 213–222.

[13] R. C.Merkle, “Protocols for public key cryptosystems,” in *Proc.of IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1980.

[14] D Kyriazis, A Menychtas, G Kousiouris, K Oberle, T Voith, M Boniface, E Oliveros, T Cucinotta, S Berger, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010

[15] Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.