JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

Facilitating Security Using Third Party Auditing Based on Fragmentation

K. Sekar[1*], G.V. Ramesh Babu[2], Sasidhar Sake[3]

[1]Dept. of Computer Science, SVUCCMCS, Sri Venkateswara University, Tirupati
[2]Dept. of Computer Science, SVUCCMCS, Tirupati
[3]Department of CSE, JNTUA, Anantapuramu

Corresponding Author: sekar_sangam@yahoo.com

DOI: https://doi.org/10.26438/ijcse/v7si6.9194 | Available online at: www.ijcseonline.org

Abstract-In Cloud computing, which is a evolving technology, security requirement is very essentials when the services are provided by the third party venders.This paper concentrates on a well-connected association between secure cloud storage and network coding. To overcome the problem of old cryptography encoding and to provide cloud surroundings with a reliable third party. This can prevent the possibility of all information about getting hacked at one time and additionally provides access management and safe removal file. Homomorphic digital signature makes use of better technology to facilitate access to authorized users only. The proposed protocol is highly economical and provides a reasonable intrusion from an anonymous party. Hence, the overall outcome expected from these tasks is to provide information access to cloud environments. The proposed systems reduce the time required to secure the new systematic structure of the Cloud Storage Protocol and provide security in uploading and downloading files.

Keywords: Cloud storage auditing, network coding, security, fragmentation, user anonymity, third-party public auditing

I. INTRODUCTION

Cloud computing, which is connected with developing technology, requires a lot of security when playing a third party as a service supplier. This paper concentrates on a well-connected association between secure cloud storage and network coding. To overcome the problems of old cryptic encoding by provide cloud surroundings with third-party credibility. This can prevent the possibility of all information about getting hacked at one time and additionally includes access management and secure file removal. Homomorphic digital signature utilizes high technology, available only to authorized users. The proposed protocol is highly economical and offers reasonable intrusion from the anonymous party. Therefore, providing access to cloud environments is the overall outcome of these tasks. The proposed systems have reduced the time needed to preserve the new structural structure of the cloud storage protocol and provide security in uploading and downloading files.

Purchasing or leasing the providers' storage capacity to store customer, company or application data. Cloud storage services can be obtained through a co-funded cloud computing service, providing the Web Service Application Programming Interface Application Programming Interface (API) Store and Forward Mode. Encoding enhances network performance for multicast tasks .In the linear coding, the router can send and receive the data packets using linear combination which increases the efficiency of data transmission. This is very applicable in case of cooperative networks [10]. Clear identities are the characteristics that identify a person. E.g., name, signature, security IDs, etc. A sensitive identifier is a good value. The attribute value cannot be found by anyone here. The banking data have been placed in the cloud info is easy and efficient to share. We can learn the information with the support of AES (“Advanced Cryptography Standard”) algorithmic program.

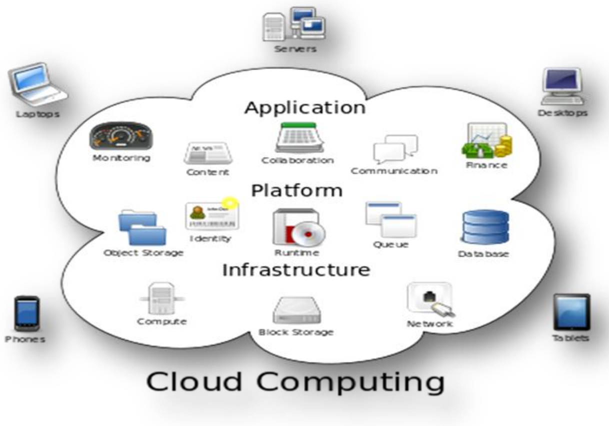


Fig 1.1: Structure of cloud computing

The rest of the paper is maintained as follows: Section 2 provides the relevant work. The proposed approach explained in section three. Chapter 4 presents an evaluation of the proposed method. Section 5 represents the conclusion.

II. RELATED WORK

Phi Chen, Tao Jiang, Yuyuan Yang, and Sherman SM. Chou [1] This paper reveals an internal interaction between cloud storage, including protected network coding. The secure cloud storage is an evolving technology and it has been eloborated over ten years in the coding community. We are showing how to equip a comfy cloud garage protocol, which provides a comfortable community coding protocol, even though two areas are pretty exceptional and independently studied in their nature. This will increase systematically to assemble flexible cloud garage protocols. Despite, outsourcing data leads to severe security matters for third-party administrative control [2].Data losses can occur because of attacks by different users and machines in the cloud. The Cloud Service Provider had another problem, i.e., Cloud Computing is a sophisticated technology that has been demanded worldwide [3].This is one of the essential things researching today. One of the best service of the cloud computing is cloud storage. In the cloud, the data has been stored in multiple servers but in the traditional networks the data stored in dedicated server. The client does not know either information put away on the different outsider servers or not and does not comprehend that the information has been spared accurately. It is managed by the Cloud Storage Provider that can save data, but no one can trust them. The data flowing through the information is stored in a network cloud in a security threat and a useful text format.

This paper presents a shorter encryption scheme with the mediation certificate without having to combine operations to share the stereotyped statistics safely in public clouds [4]. Mediated certificate-less crucial public encryption (MCL-PKE) important identity encryption and identification of certificates in identification keys Identifying the escrow issue is a significant issue. However, existing approach MCL-PKE adopts expensive pairing algorithms or attacks related to partial decryption.

Using cloud storage, users can buy their information and experience remotely from the Configurable Computing Assets Alliance pool without the burden of the nearby statistics garage and reconstruction. However, the fact that the physical ownership of outsourced statistics does not exist for consumers makes statistical integrity and significant computing in cloud computing, particularly for users with persistent computing resources [6].

III. PROPOSED WORK

Cloud computing conflicts with privacy and security issues. Privacy technologies solutions for cloud computing should provide access to privacy standards and set appropriate protection levels. Provide a stronger protection by organizations and agencies for personal information without the environment where information is kept. Disclosure of the sensitive information plays a negative impact on the organizations. Analogization may be a practical technique for achieving cloud computing. This limits the use of confidential information.

A Network coding technique is employed in network security system which includes the three entities: Sender, receiver and router. A few of the senders in the receivers group is interested to participate in broadcast. The publisher transmits data packets through the network with a simple combination of packets [7]. The router in the network also transmits the linear combination of packets which actually received for its next hop. Whenever the receiver receives the encoded data, the original data is decoded by using the actual linear system.

It can avoid a malicious router without modifying the package; each data packet sends some verification information. Whenever a router receives a packet sequence, then the router first consolidates their activation, then combines the related packages and then combines the compound packet with the combined authentication information. The Combined authentication information is calculated as according to the specific protocol's specifications.

The Secure Network Coding (SNC) protocol contains useful algorithms:

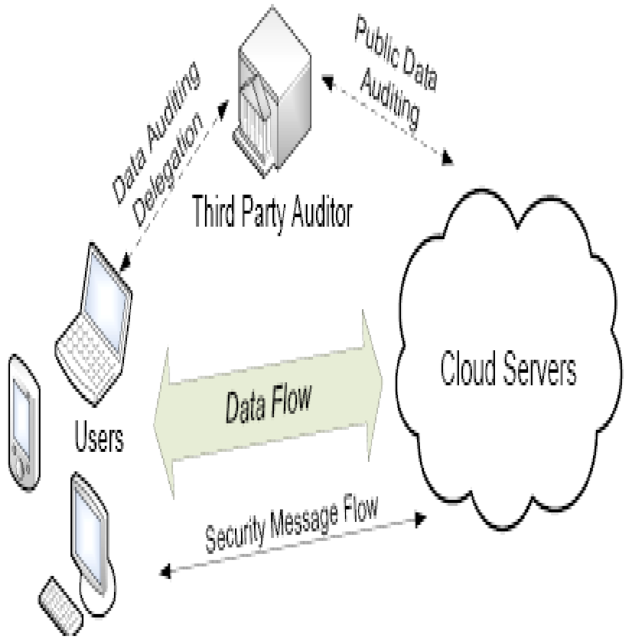


Fig 2: Secure Cloud Storage

The proposed model of a secure cloud storage system is depicted in in Fig1.There are two companies: the user and the cloud. In practice, the customer may be an individual, a group or a company using a PC or mobile phone. The cloud can be any CSP, e.g., Dropbox, Amazon S3, Google Drive, etc. Data in the cloud. Subsequently, the user maintains the audit of the integrity of outsourced data periodically. Then the user can understand whether the user is intact or not, that is, data is entire, or that data can take on evidence that could result in further action, such as legal data action or data recovery. Similar to previous work [3], and as an inspiration in the paper, we change the cloud as potentially harmful. We assume that the data conversation between the cloud and user is consistent and is performed by standard approaches. Hence, we can concentrate our attention on the customer and the cloud but not the communication.

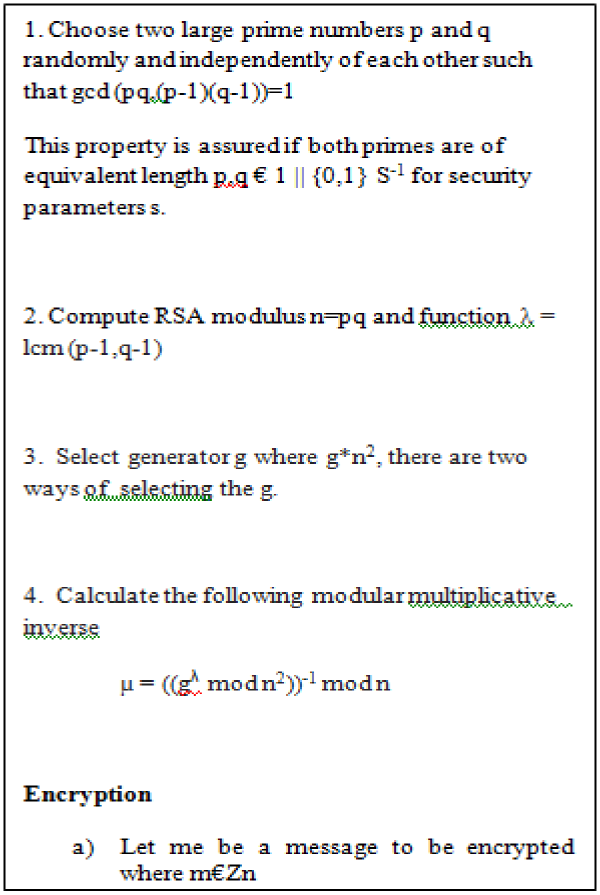
IV. PERFORMANCE ANALYSIS

In this scheme, we present security for data stored in the overlay using data stored in AES (advanced encryption standard) and inaccurate methods in the cloud. The experimental analysis is carried out in the private cloud. In future we planned to conduct in a hybrid or a public cloud can be used with some amortized efficient anonymization algorithms. An anonymization method depends on many circumstances. Otheranomalization algorithms run in addition to billing, splitting, swapping, and random noise. The existing area unit for anomalization may now be a future failure. However, information is a viable solution to indicate security in the anonymous cloud. Thus, the techniques given by anomalization are also combined to understand the results better. An efficient tool that helps in anonymization develops the integration of improved anomalization techniques.

AES Algorithm:

AES (“Advanced Encryption Standard”) is utilized for information encryption, and decryption. It is a block cipher with size of 128 bits. It permits three distinctive key lengths, in particular 128,192 or 256 bits. It is a bit based substitution approach, in each round row by step permutation performed; mixing is done in column wise and round key. AES provides encryption and verification and the encrypted data is accessed through the secret key. Using AES encryption and decryption, we may encrypt data or data that we need. Data confidentiality permits only the user with the power of data anonymization technology.

Key Generation:



1. Choose two large prime numbers p and q randomly and independently of each other such that gcd (pq,(p-1)(q-1))=1

This property is assured if both primes are of equivalent length p,q € 1 || {0,1} S^{-1} for security parameters s.

2. Compute RSA modulus n=pq and function λ = lcm (p-1,q-1)

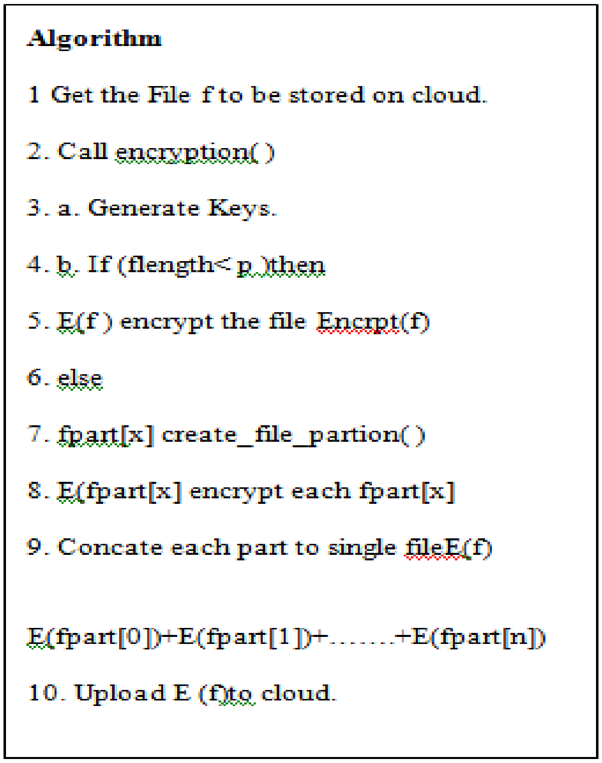
3. Select generator g where g^*n^2, there are two ways of selecting the g.

4. Calculate the following modular multiplicative inverse

$$\mu = ((g^{\lambda} \bmod n^2))^{-1} \bmod n$$

Encryption

a) Let me be a message to be encrypted where m€Zn



Algorithm

```
1 Get the File f to be stored on cloud.

2. Call encryption( )

3. a. Generate Keys.

4. b. If (flength< p )then

5. E(f ) encrypt the file Encrpt(f)

6. else

7. fpart[x] create_file_partion( )

8. E(fpart[x] encrypt each fpart[x]

9. Concate each part to single fileE(f)


E(fpart[0])+E(fpart[1])+.......+E(fpart[n])

10. Upload E (f)to cloud.
```

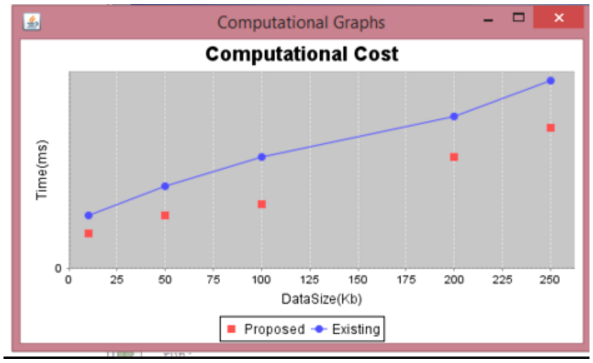


Fig 3: Graph showing Computational cost for Existing and Proposed System

V. CONCLUSION

Using third-party auditing files can get more privacy in cloud storage. We have increased our genetic structure to support username and third-party public auditing.

REFERENCES

[1] Fei Chen, Tao Xiang, Yuan Yang, Sherman S. M. Chow "Secure Cloud Storage Meets with Secure Network Coding" IEEE INFOCOM 2014- IEEE Conference on Computer Communications, 978-1-4799-3360-0/14/.

[2] Mazhar Ali, Saif U. R. Malik, Samee U. Khan," DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party," IEEE Transaction on journal name, manuscript ID IN 2015.

[3] Arjun Kumar, Byung Gook Lee, HoonJae Lee", Secure Storage and Access of Data in Cloud Computing" 978-1- 4673-4828-7/12/$31.00 ©2012 IEEE.

[4] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, and Elisa Bertino," An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Transaction on knowledge and data engineering VOL. 26, NO. 9, SEPTEMBER 2014.

[5] A. Juels and B. Kaliski Jr, "PORs: Proofs of retrievability for large files," Proc. ACM Conf. Comput.Commune. Security, pp. 584-597, 2007.

[6] Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou," Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," IEEE Transaction onparallel and distributed system, VOL. 25, NO. 1, JANUARY 2014.

[7] International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 128 ISSN 2229-5518 IJSER © 2013 http://www.ijser.org "The impact of different MAC protocols for Network Coding in Adhoc Network."

[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

[10] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–1216, 2000

Authors Profile

Mr.K.Sekar(Koneti Sekar) obtained his Bachelor Degree in Computer Science from Sri Venkateswara University. Then he obtained his Masters Degree from University of Madras and pursuing Ph.D in Sri Venkateswara University. Currently He is Professor working in the Department of Computer Science and Engineering, S.V.College of Engineering, Tirupati. His Specializations include Software Engineering, Computer Programming, Computer Security, Computer Organization and Object Oriented Programming

Dr.G.V.Ramesh Babu obtained his Bachelor Degree in Computer Science from Sri Krishnadevaraya University. Then he obtained his Masters Degree from Osmania University and obtained his doctorate degree in Sri Venkateswara University. Currently He is Assistant Professor working in the Department of Computer Science, S.V.U College of Commerce Management and Computer Science, Tirupati. His Specializations include Software Engineering, Data Mining, e-commerce, Network Security.

Sasidhar Sake obtained his Bachelor Degree in Computer Science from Rajeev Gandhi Memorial College of Engineering & Technology. Then he obtained his Masters Degree from Sir C.V. Raman Institute of Science & Technology. Currently He is working in JNTUA, Ananthapuramu.