Juni Khyat
(UGC Care Group I Listed Journal)
ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

IMPROVING SECURITY USING FRAGMENTATION-BASED THIRD PARTY AUDITING

VUTTI NARAHARI
Assistant Professor
narahariv.alts@gmail.com

A. SANDHYA RANI
Associate professor
sandhyarani1203@gmail.com

VASANTHKUMAR P A
Assistant Professor
vasanthkumaralts@gmail.com

Abstract-When acting as a third party service provider, cloud computing, which is connected to evolving technology, calls for a lot of security. This research focuses on a solid connection between network coding and safe cloud storage. to solve the issue with outdated cryptographic encoding and to provide cloud environments a trustworthy third party. The risk of all information being compromised at once may be avoided, and access control and secure file disposal are also provided. Homomorphic digital signatures make use of more advanced technologies to make access possible for only authorized users. The suggested methodology offers a reasonable intrusion from an anonymous entity and is very cost-effective. As a result, providing information access to cloud environments is the general goal of these jobs. The suggested technologies shorten the time needed to protect the Cloud Storage Protocol's new systematic structure and provide security while uploading and downloading data.

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

I. INTRODUCTION

When acting as a third party as a service provider, cloud computing, which is linked to emerging technology, calls for a lot of security. This research focuses on a solid connection between network coding and safe cloud storage. to give cloud environments with third-party credibility in order to solve the issues with previous cryptic encoding. This also incorporates access control and secure file deletion, which may stop the danger of all information being compromised at once. Homomorphic digital signatures make use of sophisticated technology that is only accessible to authorized users. The suggested methodology is very cost-effective and allows for a manageable amount of intrusion from the anonymous party. The cumulative result of these activities is to provide access to cloud environments. The time required to retain the new cloud storage protocol hierarchical structure and to guarantee security for file uploading and download has been decreased thanks to the suggested solutions. Purchasing or leasing the storage space from the supplier to keep consumer, business, or application data. A co-funded cloud computing service that offers the Store and Forward Mode Web Service Application Programming Interface (API) may be used to access cloud storage services. Network performance for multicast operations is improved by encoding. It is possible to boost efficiency by using liner coding, in which the router transmits a linear combination to receive data packets. Particularly in cooperative networks [10], this is helpful. A person may be recognized by their distinct identities. Name,

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

signature, security IDs, etc., as examples. An effective value is a sensitive identifier. No one here can locate the attribute value. The cloud-based storage of financial information makes it simple and effective to exchange. The AES (Advanced Cryptography Standard) algorithmic software aids in our knowledge acquisition.

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. Finally, Ends up Section 5 with a conclusion.

II. RELATED WORK

Sherman SM. Chou, Phi Chen, Tao Jiang, Yuyuan Yang, and others [1] This article exposes an inherent link between secured network coding and cloud storage. In the coding community, secure cloud storage has been investigated lately and for more than 10 years. We demonstrate how to set up a pleasant cloud storage protocol that offers a comfortable community coding protocol, despite the fact that the two domains are rather distinct and separately researched by their very nature. This will gradually expand to build adaptable cloud storage techniques. However, outsourcing data creates serious security issues for administrative oversight by external parties [2]. Attacks by various people and cloud-based computers might result in data loss. Another issue that the cloud service provider faced was that cloud computing is a sophisticated technology that is in high demand all over the globe [3]. One of the most important topics under investigation right now is this. The finest cloud computing services are in cloud storage. As opposed to a dedicated server used in traditional network data storage, data in the cloud is kept on a few third-party servers. The user is unaware of whether or not the data has been saved successfully and if it has been stored on any of the several third-party servers. It is run by a cloud storage provider that has the ability to preserve data, but nobody can rely on them. The information is kept in a network cloud in both a text format that poses a security risk and one that is beneficial. In order to communicate stereotyped statistics securely in public clouds, this study offers a condensed encryption approach using the mediation certificate [4]. Important identity encryption and certificate identification using mediated certificate-less vital public encryption (MCL-PKE) The main problem is figuring out the escrow issue. Existing MCL-PKE protocols, however, make use of costly pairing processes or partial decryption attacks. Without having to deal with the hassle of the local statistics garage and reconstruction, customers may purchase their knowledge and expertise remotely from the Configurable Computing Assets Alliance pool using cloud storage. However, statistical integrity and substantial processing in cloud computing are made possible, especially for customers with persistent computing capabilities, by

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

the fact that consumers do not physically possess outsourced statistics [6].

III PROPOSED WORK

Cloud computing interferes with concerns about security and privacy. Cloud computing privacy technology should make access to privacy standards available and provide the proper degrees of protection. Give personal information held by organizations and agencies greater protection without affecting the environment in which the information is stored. Organizations suffer as a result of this sensitive information. Analogization could be a useful method for implementing cloud computing. This restricts how sensitive information is used.

A example system using a network coding approach is demonstrated by network security. Entities come in three different categories: sanders, routers, and receivers. The group of senders to the receiver would want to broadcast, in certain cases. The publisher divides the data into packets and transmits them via the network in a straightforward arrangement [7]. The network's router additionally transmits a linear combination of the data packets it has just received for the subsequent hops. The receiver may decode the original data by restoring the true linear system after they receive data packets that have been properly encoded. Without altering the package, it can avoid a rogue router since every data packet transmits some verification information. When a router packet gets a sequence, the router first verifies that the packets are activated. Then it combines the appropriate packages, the combined packet, and the combined authentication data. The particular protocol's requirements are used to calculate the combined authentication information.The Secure Network Coding (SNC) protocol contains useful algorithms:

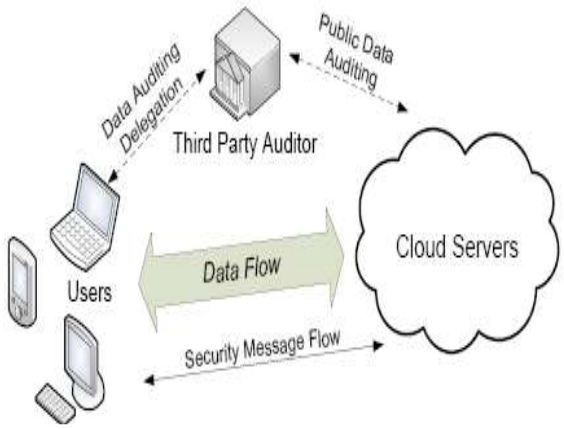

Fig 2: Secure Cloud Storage

As shown in Fig. 1, we model a safe cloud storage system. The user and the cloud are two separate businesses. In actuality, the consumer may be a person, a group, or a business utilizing a computer or a mobile phone. Any CSP, such as Amazon S3, Dropbox, Google Drive, etc., may serve as the cloud. data stored online. As a result, the user continues to regularly check the integrity of data that has been outsourced. The user will then be able to determine if the user is whole or not, meaning that the data is complete, or whether the data contains evidence that may warrant taking additional action, such as legal action or data recovery. In keeping with earlier research [3] and as a motivation for the article, we reframe the cloud as potentially dangerous. We presume that the user's communication with the cloud is standardized and conducted using established procedures. As a result, we can focus on the client and the cloud but not on the communication.

IV PERFORMANCE ANALYSIS

With the help of faulty cloud-based technologies and data saved in the advanced encryption standard (AES), we offer security for data stored in the overlay in this scheme. Currently, the private cloud will

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

be used for experimental analysis. In the future, more effective anonymization methods may be utilized with a public cloud or hybrid cloud. A technique of anonymization is dependent on a variety of factors. In addition to billing, splitting, swapping, and random noise, further anomalization methods are used. The area unit for anomalization that is now in use could fail in the future. Information, however, is a workable way to show security in the anonymous cloud. In order to better comprehend the outcomes, the approaches provided by anomalization are also incorporated. An effective anonymization tool promotes the incorporation of enhanced anomalization methods.

The Advanced Encryption Standard (AES) algorithm is used to encode and decode data. It is a 128-bit black cipher block cipher. It supports keys with lengths of 128, 192, or 256 bits. a bit-based replacement that is compatible with the round key, column-wise mixing phase, and row-by-step permutation throughout each round. AES offers encryption and verification services and holds the secret key needed to decrypt data. We may encrypt data or anything that we require using AES encryption and decryption. Only users with access to data anonymization technologies are allowed to maintain data confidentiality.

Key Generation:

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

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

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

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.

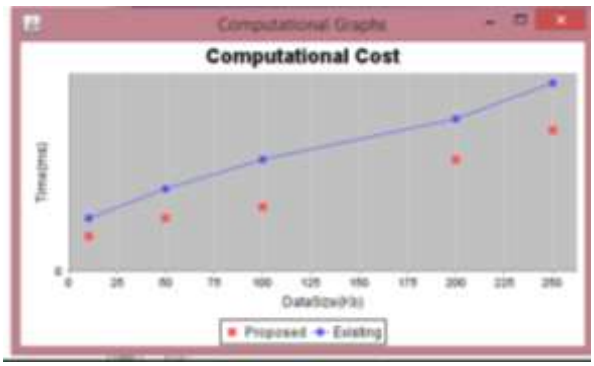

Fig 3: Graph showing Computational cost for Existing and Proposed System

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.

ISSN: 2278-4632
Vol-10 Issue-2 No.01 February 2020

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.