A Survey On Data Integrity Checking and Enhancing Security for Cloud to Fog Computing

[1]Dr. Shital Agrawal, [2]Mr. Digvijay Devare, [3]Mr. Shubham Gotarne, [4]Miss. Priti Patil.
[1]Asst.Professor,[2,3,4]UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharashtra, India.
[1]shital.s.agrawal@gmail.com, [2]digvijaydevare@gmail.com, [3]shubhamgotarne1@gmail.com, [4]pritipatil12527@gmail.com

Abstract - In accordance with its ability to supply services to users via the internet at a lower cost, cloud computing is becoming more and more essential in the computer world. Cloud service providers (CSPs) relieve clients of the hassle of managing their data and provide massive amounts of storage space at very low costs. The lack of transparency in the operational details may make the CSPs untrustworthy. They might copy data to conceal data loss, alter data, remove infrequently accessed data, or steal user data. When this happens, data integrity breaks and needs to be fixed. The cloud platform is expanded by the upcoming fog computing paradigm to offer services for Internet of Things applications. Thus, in addition to being integrated into cloud computing, data integrity verification approaches are also being expanded for fog computing. The many approaches to verify data integrity in cloud and fog environments are covered in this survey.[1]

Keywords: Fog Computing, Cloud computing, Security, Privacy, psychometric test, Profile behavior techniques.

I. INTRODUCTION

Decentralized fog computing reduces data transmission costs and improves cloud platform performance by minimizing needless data processing and storage by processing information closer to its source

before it reaches the cloud. This strategy is motivated by the growing number of Internet of Things gadgets that are producing enormous volumes of data, which calls for the processing of data and fast decision-making in order to preserve optimal performance. When data is managed by the server and received by the client in a normal client-server architecture, there may be issues with scalability and dependability.[1] The Fog paradigm provides an effective means of data processing, transmission, sorting, grouping, and examination by creating a hierarchically dispersed platform that sits between end-user devices and the cloud system. With the goal of improving system performance and saving communication resources, Cisco officially announced this novel technique, called fog computing.[3]

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is considered one among the foremost promising techniques. A salient feature of CPABE is that it grants data owners direct control power supported access policies, to supply flexible, fine grained and secure access control for cloud storage systems. A salient feature of CPABE is that it grants data owners direct control power supported access policies, to supply flexible, fine grained and secure access control for cloud storage systems. An owner's data is encrypted with an access structure over attributes, and a user's secret key's labelled

with own attributes, as long as the attributes. [8]

II. AIMS AND OBJECTIVE

a) Aim

The primary aim of the project is secure a data integrity checking to explore the technique. Also Enhancing security to investigate the security fog computing.

The data integrity in the frame of reference of security is to ensure that data remains accurate, complete, and reliable throughout its lifecycle. Data integrity is a fundamental component of data security, and it is essential for securing data from various threats, such as unauthorized access, tampering, corruption, or data breaches. These measures help safeguard data from threats, ensure its accuracy, and maintain its trustworthiness, contributing to an overall robust security posture.

b) Objective

1. Data entry The process of turning a user-focused input description into a computer-based system is called design. This design is crucial to avoiding data entry errors and providing management with the right guidance on how to obtain accurate information from the computerized system.

 DOI : 10.35291/2454-9150.2024.0251 © 2024, IJREAM All Rights Reserved.

2. The creation of user-friendly data entry panels allows for the handling of enormous volumes of data. Ensuring error-free data entering is the objective of input design. All data manipulations are possible thanks to the design of the data entering page. It also offers facilities for viewing records.

3. A validity check will be performed on the data upon entry. Screens are useful for entering data. So that to prevent the user from being lost in the moment, pertinent notifications are given as needed. Making an input layout simple to understand is, therefore, the goal of input design.

III. LITERATURE SURVEY

Paper 1: A Survey on Enhancing Cloud Security Using Fog Computing

This article introduces fog computing, which has grown to be a significant field of study within the cloud computing industry. because it can elongate cloud services to the network's edge and because of its ability to lower latency and increase QoS, all of which improve user experience. Fog computing's characteristics, however, provide additional security and protection problems. Because of its mobility and heterogeneity, fog computing cannot be simply categorized under the current security and protection estimates for cloud computing. Thus, these problems with fog computing present new chances and difficulties for study. This review covers current security problems for fog computing and a newly suggested approach to address some of the privacy and security issues in fog computing, improving the cloud.[2]

Paper 2: Scalable pCT image reconstruction delivered as a cloud service.

This article compares the performance of the identical application operating on dedicated local high performance computing resources with our pCT reconstruction service running on commercial cloud resources. Provide an on request, multiple user providing service that can handle episodic demand by dynamically resizing and supplying clusters in response to priorities, wait times, and image reconstruction requirements. They make use of GPU-enabled cluster resources from Amazon Web Services, which are equipped with high-speed networks connecting nodes, in order to meet the application's high performance needs. Because of the nature of proton treatment, there may be hundreds of clients globally who occasionally require this kind of service. The utilization of a commercial cloud as scalable and affordable platform for pCT remodeling is examined in this paper.[4]

Paper 3: Integrity Checking Using Third Party Auditor in Cloud Storage

This article cloud computing one of the quickly growing technologies in the globe that offers its consumers a variety of services. Storage as a Service is a popular service provided by the cloud to its clients. This service relieves the user of the task for maintaining and storing content by enabling him to move his data to a distant storage server and access it from any location. The cloud stores, handles, and backs up the user's data, which is then made available to him web. However, the privacy and integrity of stored data are the primary concerns while utilizing this kind of service. An attacker may able to access, alter, or destroy data that is stored remotely. Users want data to be protected from these kinds of unwanted actions; hence, data integrity verification procedures are required to determine whether or not the stored files are unchanged. Because the user does not have immediate access to the data, integrity verification is a difficult process. The proposed approach uses bilinear pairing to have a third-party auditor verify the accuracy of data kept at a remote site. Aggregation is then used over the suggested method for additional optimization. [5]

IV. EXISTING SYSTEM

Due to their cryptographic nature, current in cloud data integrity validation techniques are not appropriate for fog environments. Therefore, a simple strategy to check the data integrity in the fog environment is required. Because the data is not under the user's control, cloud storage presents security concerns related to confidentiality, availability, and integrity even though it lowers capital costs, application deployment times, and information administration and maintenance.[1] To improve efficiency of this encryption technique, Emera et al. proposed a CP-ABE scheme with a continuing ciphertext length. Subsequently, some cryptographically stronger CP-ABE constructions but these schemes imposed some restrictions that the original CP-ABE does not have. In , Waters three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive .[8]

V. COMPARATIVE STUDY

Table 1 . Comparative Analysis

Sr. No	Author's	Project Title	Publication	Purpose
1	K.Uma Maheswari , S.Mary Saira Bhanu , S.Nickolas	A Survey on Data Integrity Checking and Enhancing Security for Cloud to Fog Computing	IEEE, 2020	It offers a cheap way to delivering clients with services via the internet.

 DOI : 10.35291/2454-9150.2024.0251 © 2024, IJREAM All Rights Reserved.

2	Prasad K. D, Mandhar D, Arpit B, Abhi A. S	A Survey on Enhancing Cloud Security Using Fog Computing	**RESEARCHGATE, 2020**	Cloud services towards the edge of the network, reduced service latency and improved Quality of Services.
3	Chard, Ryan, Ravi Madduri, Nicholas T. Karonis	Scalable pCT image reconstruction delivered as a cloud service.	**IEEE, 2020**	Local high performance computing resources with service running on cloud resources.
4	Chakraborty Sutirtha, Sr. Shubham Singh Albert, Surmila Th.	Integrity Checking Using Third Party Auditor in Cloud Storage	**RESEARCHGATE, 2018**	Provides a range of services to its clients. Storage as a Service (STaaS) It has the most popular salient services that the cloud offers.

VI. PROBLEM STATEMENT

In cloud computing, Because the data poses an increased risk to security, access to fog services and data via the Internet points out the importance of security.[6] By entrusting their data to an external source, users no longer have the burden of storing data locally, which relinquishes control from the owner. This situation poses challenges in protecting data security and raises concerns regarding data security, particularly for users with limited capabilities and resources for computing. The article proposes a method to ensure the security of data stored on a remote cloud server to ensure the accuracy of data saved on a remote server by involving a third-party auditor, and also utilizes aggregation to enhance the efficiency of the system. [1]

VII. PROPOSED SYSTEM

The main goal of this research is to examine the different methods used for verifying data security in cloud and fog environments through authentication structures, as well as to assess their limitations. These methods are categorized as root signature based, BF based, tag regeneration based, and table-based schemes. The investigation concludes that root signature-based approaches are appropriate for verifying integrity in a single instance of dynamic data, BF-based methods are suitable for a single instance of static data, tag regeneration-based techniques are ideal for IoT data, and table-based schemes are best suited for verifying integrity in multiple instances of dynamic data.[1] A technique for providing transfer of data in a fog computing environment by sending data where it requires the most, relying to the needs of various users. Both data consumers and data suppliers may own data storage systems. [7]

VIII. ALGORITHM

The general idea of working of proposed system algorithm as follow:

Encryption Algorithm:-

1. Key key ← generateKey();
2. Cipher c ← Cipher.getInstance(ALGO);
3. c.init(Cipher.ENCRYPT_MODE, key);
4. byte[] encVal ← c.doFinal (Data.getBytes());
5. String encryptedValue ← new BASE64Encoder().encode(encVal);
6. return encryptedValue;

Decryption Algorithm: -

1. Key key ← generateKey();
2. Cipher c ← Cipher.getInstance(ALGO);
3. c.init(Cipher.DECRYPT_MODE, key);
4. byte[] decordedValue ← new BASE64Decoder().decodeBuffer(encryptedData)

5.byte[] decValue ← c.doFinal(decordedValue);

6 String decryptedValue ← new String(decValue);

7. return decryptedValue;

IX. MATHEMATICAL MODEL

F = (m1, . . . ,mn)∈ℤp user´s data which should be stored in the server storage where n is the No. of blocks and p is a high prime number.

fkey(·) – pseudorandom function (PRF), defined as:

$\{0, 1\} \ast\times key \rightarrow \mathbb{Z}p.$

πkey(·) – pseudorandom permutation (PRP), defined as:

$$\{0,1\}^{log2(n)} \times key \rightarrow \{0,1\}^{log2(n)}$$

MACkey(·) – message authentication code (MAC) function, defined as:

$$\{0, 1\}\ast\times key \rightarrow \{0,1\}^{1}.$$

H(·), h(·) – map-to-point hash functions, defined as: {0, 1}∗ →G, where G is some group.

Let G1, G2 and GT to be the multiplicative cyclic group of line p and e: G1 × G2 → GT was a bilinear map. Let g be the generator G2.H(·) which was a secure map-to-point hash function: {0,1}∗→ G1 which mapped the integer (chains) uniformly into G1. Hash function $h(\cdot)$:G1 → ℤp mapped the element groups G1 into ℤp . The user launched the algorithm KeyGen and generated the public and private parameters. Randomly selected x ← ℤp,

 DOI : 10.35291/2454-9150.2024.0251 © 2024, IJREAM All Rights Reserved.

random element u ← G1 and calculated u ← g^x and w ← u^x. Sk=(x) was the secret parameter, while vk = (v,q,g,u) was the public one. The user used the SigGen method to determine the sign σ_i for each data block mi on the data F = (m1,...,m_n): σ_i← (H(i) · u^mi)^x ∈G1, for i=(1,...,n). Following that, Φ = {σ_i }_(1 < I ≤n)fori=(1, …, n) was the total of all signs. As consequently, the user erased the local copy and sent {F, Φ} on a server.

The server used the GenProff method to create a response as evidence of the accuracy of the data stored after receiving the message.

TAS started the algorithm Verify Proof after getting the response from the server, which calculated the answer's correctness using the verifying equation.

X. SYSTEM ARCHITECTURE

1.Key generation: To create the public and secret key, methods like linear linking are applied in this stage. These keys are a combination of multiple rules rather than being based on a single parameter.

2. File splitting: A user files are split up into blocks, which are then frequently further categorized into sectors.

3. Tag generation: Using a public key, the private key, along with some random data, a tag is created for every block or sector.

4. Creating the authentication structure: The authentication structure is created using the tag values of every single block. The server

gets the file, tag values, and a part of key data.

5. TPA/User challenges the server: By transferring random block indices, a verifier creates problems on thewebserver.
6. Generation of proof: In response, the server creates proof data and passes it to the validator.

7. Verifiability of the evidence: The TPA uses the information saved from the files to confirm the proof.

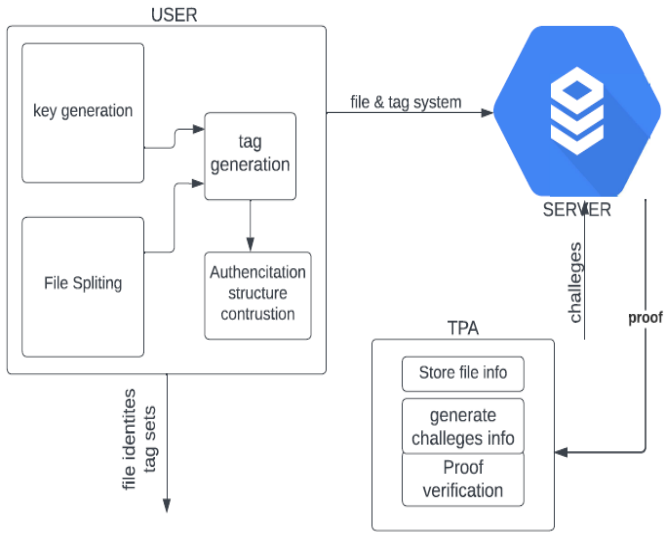

Fig.1: System Architecture

XI. ADVANTAGES

- Effective Data Management: End-user data can be reduced, controlled, and organized using fog apps. The connection between a device and local network is where necessary data is gathered and analyzed.
- Enhanced Security and Privacy: Fog computing can benefit from a number of security and privacy-preserving strategies, including biometric authentication, privacy-protecting cryptology, user profiling, and behavior approaches.
- Improved Business Agility: With the right tools and methods, programmers can create fog apps quickly and implement them as needed.
- Cost Savings: Organizations may save long-term expenses related to data breaches, charges from officials, and loss to their brand by making an upfront investment in data integrity testing and safety precautions. Organizations may save costs and avoid costly incidents by anticipating security risks and maintaining data security.
- Without security key Data user cannot access the file uploaded by Data owner, when TPA generates a security key then only Data user can access the data.

XII. DESIGN DETAILS

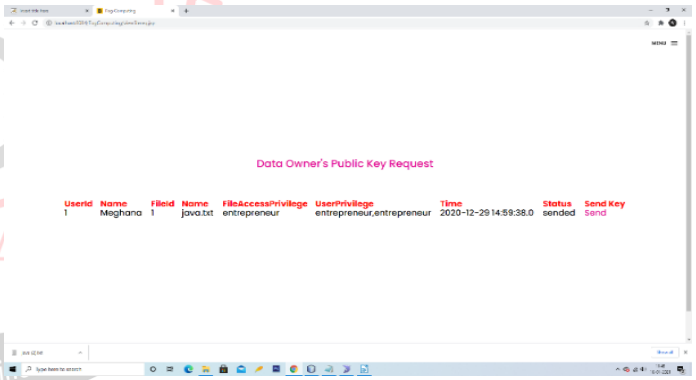

Fig 2: Result

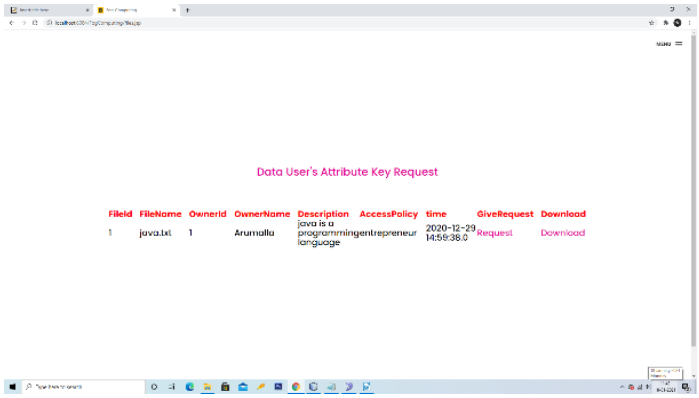

Fig 3: Result

XIII. CONCLUSION

Thus we have tried to implemented the paper "A Survey on Data Integrity Checking and Enhancing Security for Cloud

 DOI : 10.35291/2454-9150.2024.0251 © 2024, IJREAM All Rights Reserved.

to Fog Computing," , K. U. Maheswari, S. M. S. Bhanu and S. Nickolas, IEEE 2020 and the conclusion as follow: The study and assessment of the various structure-based authentication methods employed in cloud and fog environments to guarantee data integrity is the aim of this research. A taxonomy of several integrity checking techniques is presented in this study. Because they are encrypted in nature, current cloud data integrity validation methods are not appropriate for fog environments. Therefore, the requirement arises. Consequently, in order to confirm the data purity in the fog environments, an easy method is required. In the future, an efficient protocol for integrity testing and retrieving data that is inaccurate in the fog environment will be proposed, based on erasure coding methods to prevent data loss.

REFERENCE

[1] K. U. Maheswari, S. M. S. Bhanu and S. Nickolas, "A Survey on Data Integrity Checking and Enhancing Security for Cloud to Fog Computing," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 121-127, doi: 10.1109/ICIMIA48430.2020.9074890.

[2] B, Arpit & D, Prasad & D, Mandhar & S, Abhi. (2020). A Survey on Enhancing Cloud Security Using Fog Computing. 10.31226/osf.io/4pt59.

[3] Kunal, Sourav & Saha, Arijit & Amin, Ruhul. (2019). An overview of cloud-fog computing: Architectures, applications with security challenges. Security and Privacy. 2. 10.1002/spy2.72.

[4] R. Chard et al., "Scalable pCT Image Reconstruction Delivered as a Cloud Service," in IEEE Transactions on Cloud Computing, vol. 6, no. 1, pp. 182-195, 1 Jan.-March 2018, doi: 10.1109/TCC.2015.2457423.

[5] Chakraborty, Sutirtha & Singh Albert, Sr & Th, Surmila. (2018). Integrity Checking Using Third Party Auditor in Cloud Storage. 1-6. 10.1109/IC3.2018.8530649.

[6] Munir, Kashif & Mohammed, Lawan. (2018). Secure Third Party Auditor(TPA) for Ensuring Data Integrity in Fog Computing. International Journal of Network Security 10. 10.5121/ijnsa.2018.10602.

[7] Moysiadis, Vasileios & Sarigiannidis, Panagiotis & Moscholios, Ioannis. (2018). Towards Distributed Data Management in Fog Computing. Wireless Communications and Mobile Computing. 2018. 1-14. 10.1155/2018/7597686.

[8] Prof. Swapnil wani, Javed khan, Anamika Jaiswar, Priyanka gujar “RAAC With Multiple Attribute Authority For Public Cloud” ISSN : 2454-9150 Vol-06, Special Issue, June 2020.

 DOI : 10.35291/2454-9150.2024.0251 © 2024, IJREAM All Rights Reserved.