An Approach for a Fog-centric Secure Cloud Storage Scheme

K. Anuhya, Gautam Kumar, Mrutyunjaya S. Yalawar

Abstract: Currently, cloud computing is being considered as a possible replacement for providing storage services. Security concerns with cloud storage might prevent its mainstream adoption. New security hazards to cloud storage include data breaches, malicious alterations, and data loss. For safe storage employing different clouds, a three-tier architecture built on Fog servers has recently been described. Hash Solomon's code and a specially created hash algorithm are the fundamental methods employed to accomplish the task. This does not, however, provide improved change detection and data recovery and results in the loss of a tiny amount of data to cloud servers. This research suggests a unique secure cloud storage system focused on fog to guard against illegal access, alteration, and destruction of data. The suggested strategy employs a novel method of data obscuration to prevent unwanted access. Additionally, the outcomes of Block - Management to stop unauthorised access and provide greater recovery in case of data loss. In addition, we provide a method based on a hash algorithm to make it simpler to find high-probability changes. Through security analysis, we show that the suggested approach is reliable. Experimental findings support the suggested scheme's performance advantage over modern alternatives in terms of data processing speed.

Keywords: Cloud storage, fog server, Xor-Combination, CRH, privacy.

I. INTRODUCTION

SES 2006 (Search Engine Strategies 2006) proposed CLOUD computing, a well-known computing paradigm, and NIST (National Institute of Standards and Technology) [1] gave it formal definition in 2009. With its strong computation, storage, and networking capabilities, this technology has since increased its market share [2, 3]. Its infrastructure resources can be scaled up or down as needed and are inexpensive with a convenient pay-as-you-go payment option. In addition to consumers and businesses, many research communities are paying attention to cloud computing and making significant efforts to help it gradually mature. Because of this, cloud computing has a wide range of functions, and cloud storage techniques are becoming more crucial as data volumes grow. With an increase in network bandwidth, user data volume grows exponentially [4]. Almost every internet user has access to between GB and TB of personal cloud storage. These enormous storage needs can't be satisfied by local storage alone. More crucially, individuals require constant access to their data by nature. People therefore discover new media to store their data. Users are turning to cloud storage in greater numbers as they prefer powerful storage capabilities. They also favour using the cloud to store their private data. In the not too distant future, storing data on a for-profit public cloud server will become a common practise. Numerous businesses, like Dropbox, Google Drive, iCloud, and Baidu Cloud, have drawn inspiration from this and now provide their customers with a variety of storage options. However, a number of security dangers accompany the advantages of cloud storage [5-8]. The largest concerns are data loss, malicious alterations, server breakdowns, and privacy-related problems. These are a few instances of online dangers. Three billion Yahoo accounts were compromised by hackers in 2013, Apple's iCloud leak happened in 2014, and Dropbox suffered a data breach in 2016. Of these, the iCloud leak that revealed the private photos of several Hollywood actresses stands out. a shrill cry. Such events may damage a company's image for a long time [9–10]. In conventional cloud computing scenarios, users can no longer physically protect their data once it has been offloaded to the cloud. Cloud service providers (CSPs) have access to, and may search for or change, their data that is kept in cloud storage. At the same time, technological mistakes might cause CSP to unintentionally lose data. Alternately, a hacker could compromise the privacy of user data. Certain cryptographic techniques (such encryption and hash chains) may ensure confidentiality or integrity [10]. However, no matter how much the algorithm is enhanced, the cryptographic technique cannot thwart insider assaults [9]. Several academic groups have proposed the concept of fog computing to install fog devices between the user and the cloud server in order to safeguard data privacy, integrity, and availability (CIA). Wang et alwork .'s in this field is among the most notable and recent. For the purpose of maintaining data privacy and integrity, they employed Reed Solomon code and hash digest-centric proprietary algorithms [8].Additionally, they created computational intelligence (CI) to determine how much data should be stored locally, on the cloud, and in Fog.

Manuscript received on 16 August 2022 | Revised Manuscript received on 23 August 2022 | Manuscript Accepted on 15 September 2022 | Manuscript published on 30 September 2022.
***** Correspondence Author

K. Anuhya, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India.

Dr. Gautam Kumar, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India.

Mrutyunjaya S. Yalawar*, Department of Computer Science and Engineering, CMR Engineering College, Hyderabad (Telangana), India. Email: mrutyunjaya.cmrec20@cmrec.ac.in

Retrieval Number: 100.1/ijrte.C72670911322
DOI: 10.35940/ijrte.C7267.0911322
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

To allow users to review cloud servers and ensure that the cloud servers are responsive, they maintain a rating system.

This technique demonstrates that, although requiring more compute and storage cost, some (but not all) of the data in the cloud and its bespoke hash algorithm have no advantage over the common hash algorithm (i.e. MD5) in terms of collision resistance.

We suggest a fog-based cloud storage system for data privacy, integrity, and availability in this white paper. We provide a mechanism called Xor Combination that divides the data using numerous operations/blocks utilising various clouds/blocks for privacy and availability reasons (even after harmful occurrences). The suggested method chooses a cloud server to store each specified data block in order to prevent any one cloud server from obtaining all of the original data. We suggest a fantastic hashing approach, called a Collision Resolving (CRH) procedure, which enables to obtain certain data from several sources at once. Regarding security features and hashing [9]. The suggested plan is showing promise as a reliable option for effective and secure cloud storage.

II. LITERATURE REVIEW

Academic and industry researchers are becoming more aware of the value of cloud storage. The primary study areas include enhancing cloud storage performance and preserving security standards. The emphasis of research to improve the dependability of storage systems has always been security problems [15].

The biggest cyber hazards to cloud storage, according to many study studies [16–19], are data breaches, malicious alterations (or integrity violations), and data loss. In order to address the security issues mentioned above, according to Kaufman's argument, cloud servers must implement consistent and practical regulations . Zissis et al. conducted an analysis of cloud security by defining specific security criteria and offering a conceptual solution with the help of a reliable outside party (TTP). They addressed particular issues by using public-key cryptography as the underlying cryptographic instrument to guarantee the secrecy, integrity, and authenticity of data and communications . In order to combat this, Wang et al. focused on integrity protection in cloud computing and suggested a public auditability method [2].

They had two objectives: one was to audit public accounts effectively without needing a local copy of the data, and the other was to avoid introducing vulnerabilities in the data. To secure privacy and provide open auditing of cloud data, they employed homomorphic authentication with random masking. The computational cost of public key-centric homomorphic authentication, however, is substantial, and partial/complete data loss is not the subject of this study. [4] makes a suggestion for an effective random blockless verification methodology. The key component of their suggested protocol is a magnificent dynamic data structure made up of a location array and a doubly linked information table. Costs for computing and communication are considerably decreased with this design.

In contrast, it just addresses integrity checks for cyberthreats, much as the prior plan. A technique called content-based image retrieval (CBIR), based on secure k-nearest neighbour (kNN) and locality-sensitive hashing (LSH), was suggested by Jia et al. to safeguard pictures sent to cloud servers [10]. This also holds true for other forms of data (ie text). While this assures effective recovery and protects the privacy of private photographs, it does not guarantee the integrity or removal of the image (or any other type of data). Arora and other people [5] described and contrasted a few cryptographic primitives for securing the confidentiality and integrity of cloud storage. Other computer architectures may be compared using this example. Shen et almost .'s recent work. Urbanization uses cloud infrastructure. In their idea, a cloud was proposed as a means of data sharing between users and/or programmes [2]. They employed attribute-based encryption to safeguard the privacy of shared data (ABT). However, they emphasise data security and depend on cloud servers to maintain data integrity and avoid data loss. Indeed, Khan et al. emphasise the need of cloud computing trust. In their work [7], the authors explore the difficulties with cloud trust and how a cloud server might gain the confidence of its users. The earlier studies that have been mentioned so far are typically concerned with integrity management using different public and private audit frameworks. On the other side, encryption offers the strongest privacy protection, despite the fact that it makes search more difficult. In order to search encrypted cloud data, a number of searchable encryption techniques have been developed [2–3].

Fog server-centric solutions are superior to other TTA (Third Party Auditor) based solutions in terms of thwarting cyber attacks. For instance, TTA systems offer nothing to safeguard privacy but are effective at spotting harmful alterations. Comparably, searchable encryption methods are effective at preserving privacy and allowing for (relatively) quick data retrieval, but they have drawbacks such the possibility of data loss and manipulation. A fog server, which is a cloud server extension that is located closer to the user, provides a possible defence against numerous cyber dangers. Fog-based defences against cyber attacks haven't been thoroughly researched yet, however. In order to defend against different threats, Tian et al. presented a novel cloud storage system that makes use of fog servers [1]. They inserted a fog server between the cloud server and the users, resulting in a three-tier design. Given that the user has confidence in the Fog server, they provide an excellent system to protect privacy, spot changes, and avoid data loss. To prevent any one cloud server from reconstructing the data, they encrypt the data using Reed-Solomon coding and derive computation intelligence (CI) to decide how much data to offload to cloud/fog servers. However, each outsourced cloud server receives access to a certain amount of data. As opposed to this, they create Malicious Modification Detection (MMD), which has no benefit over conventional hashing algorithms for the detection of malicious alterations.

Retrieval Number: 100.1/ijrte.C72670911322
DOI: 10.35940/ijrte.C7267.0911322
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

With the same design, a different newly presented work has accomplished the same thing.
These studies advise using fog-based systems to store data securely in the cloud and, more specifically, to guard against online attacks that target cloud data.
The authors of this study use the Tian et al. approach to develop a secure cloud storage system based on fog servers. Think of it as a standard.

III. METHODOLOGY

3.1 Existing System

Using a dependable third party, Zissis et alanalysis .'s of cloud security identified clear security needs and offered a conceptual solution (TTP). They addressed particular issues by using public-key cryptography as the underlying cryptographic instrument to guarantee the secrecy, integrity, and authenticity of data and communications [7].

In order to combat this, Wang et al. focused on integrity protection in cloud computing and suggested a public auditability method [8]. They had two objectives: one was to audit public accounts effectively without needing a local copy of the data, and the other was to avoid introducing vulnerabilities in the data. To secure privacy and provide open auditing of cloud data, they employed homomorphic authentication with random masking. In order to safeguard photos sent to cloud servers, Xia et al. introduced a technique called content-based image retrieval (CBIR) based on secure k-nearest neighbour (kNN) and locality-sensitive hashing (LSH) algorithms.

This also holds true for other forms of data (ie text). While this assures effective recovery and protects the privacy of private photographs, it does not guarantee the integrity or removal of the image (or any other type of data). Arora and other people To safeguard the confidentiality and integrity of cloud storage, a few cryptographic primitives have been described and contrasted. Other computer architectures may be compared using this example. Shen et almost.'s recent work. Urbanization uses cloud infrastructure. In their idea, a cloud was proposed as a means of data sharing between users and/or programmes. They employed attribute-based encryption to safeguard the privacy of shared data (ABT).

3.2 Proposed System

Suggested a secure cloud memory architecture based on fog computing that makes use of Xor-Combination, Block-Management, and CRH operation. The suggested scheme's privacy guarantee, data recoverability, and change detection are shown by theoretical security analysis. Implemented a prototype system scheme and conducted tests to see how it performed in comparison to the current scheme. The results demonstrate its effectiveness in terms of time and memory use.

3.3 Flowchart

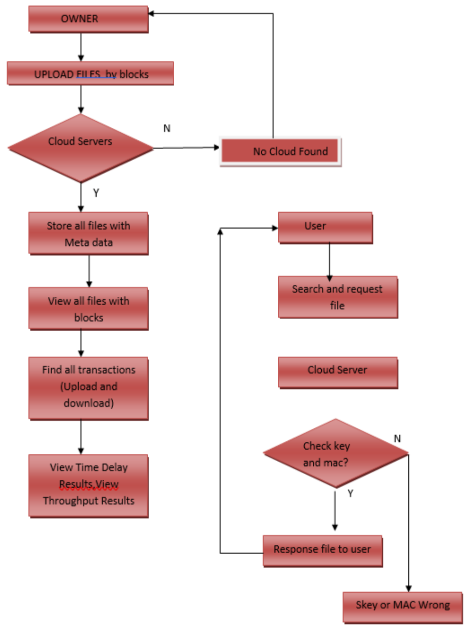


Fig.1.Flow chart 3.1 Data Flow Diagram Level -0

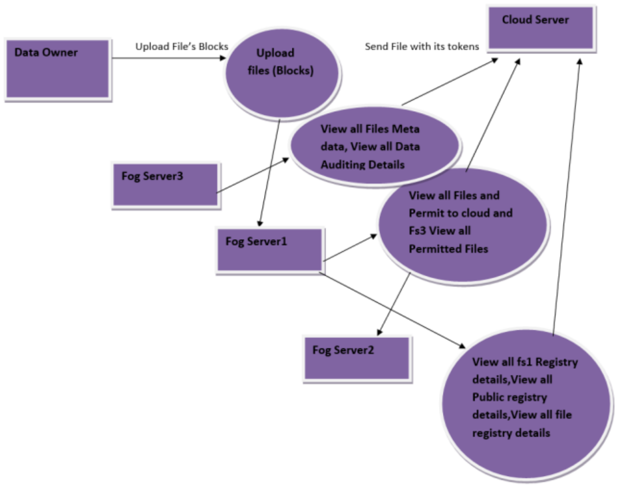

Data Owner
Upload File's Blocks
Upload files (Blocks)
Send File with its tokens
Cloud Server
View all Files Meta data, View all Data Auditing Details
Fog Server3
View all Files and Permit to cloud and Fs3 View all Permitted Files
Fog Server1
Fog Server2
View all fs1 Registry details,View all Public registry details,View all file registry details

Fig.2. Flow Diagram Level -0

Level -1

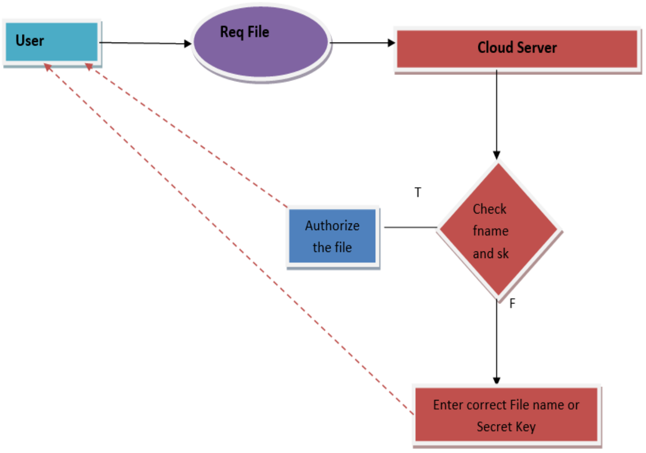


Fig.3. Flow Diagram Level -1

Level -2

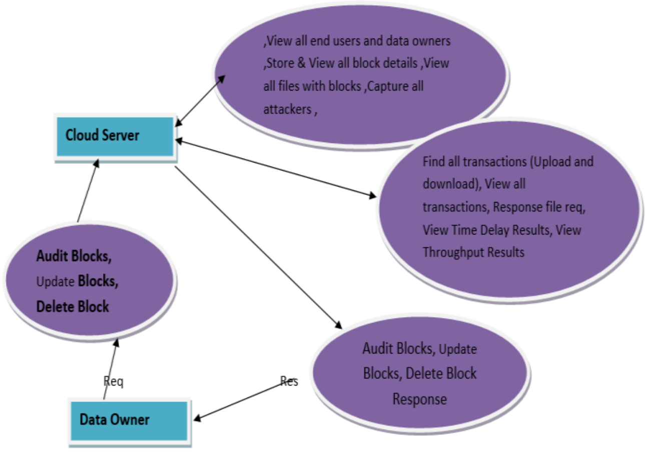

,View all end users and data owners ,Store & View all block details ,View all files with blocks ,Capture all attackers ,
Cloud Server
Find all transactions (Upload and download), View all transactions, Response file req, View Time Delay Results, View Throughput Results
Audit Blocks, Update Blocks, Delete Block
Audit Blocks, Update Blocks, Delete Block Response
Req
Res
Data Owner

Fig.4. Flow Diagram Level -2

IV. IMPLEMENTATION

User: The ultimate objective of this document is data security, disaster recovery, and user data modification detection.

FogServer: The user is used to Fag Server. The user gets their info from the Fog server. Fog server dependability to the user is ensured by proximity of fog devices to the user, robust physical security, correct authentication, secure communications, and intrusion detection.

CloudServer: The cloud server is seen to be trustworthy but intrepid. This indicates that although the cloud server is correctly adhering to the Service Level Agreement (SLA), it also plans to analyse user data. A cloud server, in contrast, presents itself as an ally while really acting as a potential foe. In this scenario, the data may be altered by the cloud server and misrepresented as the original data. Similar to how the user may lose their data permanently if the cloud server loses or hides data. Data tampering or irreversible loss may also be the consequence of hardware or software failure.

V. RESULTS

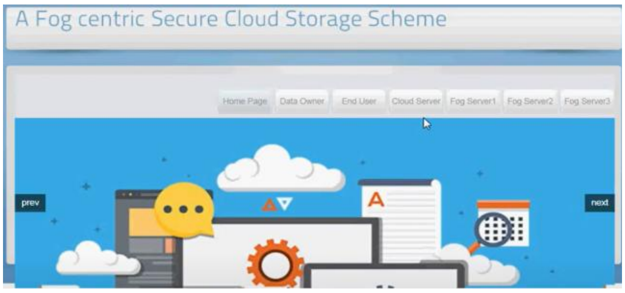
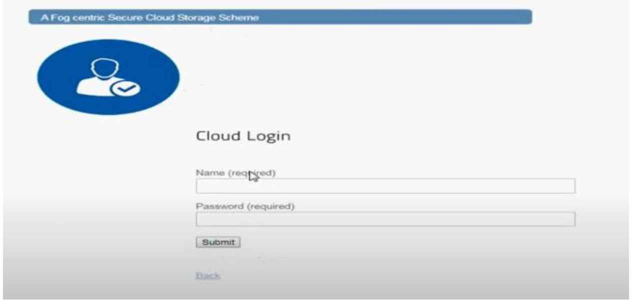

A Fog centric Secure Cloud Storage Scheme

Fig.5. Home

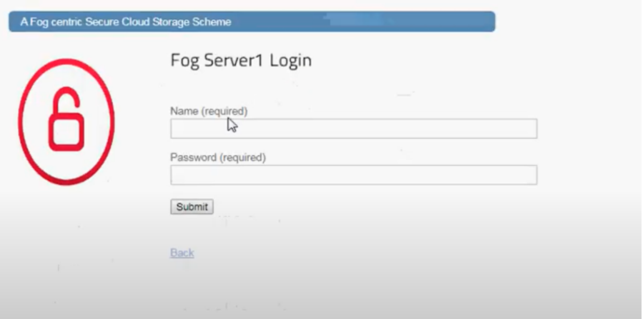

A Fog centric Secure Cloud Storage Scheme

Cloud Login

Name (required)

Password (required)

Fig.6. Cloud Login

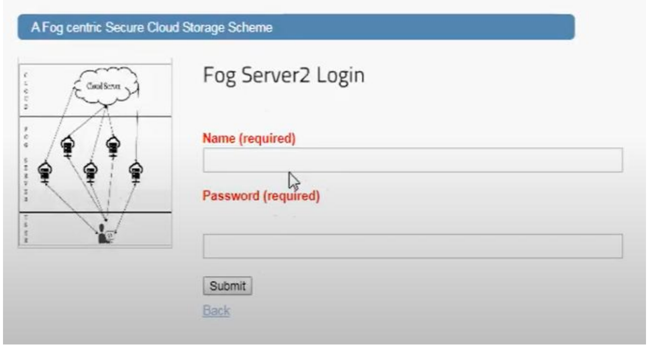

A Fog centric Secure Cloud Storage Scheme

Fog Server1 Login

Name (required)

Password (required)

Fig.7. *FogServer* Login 1

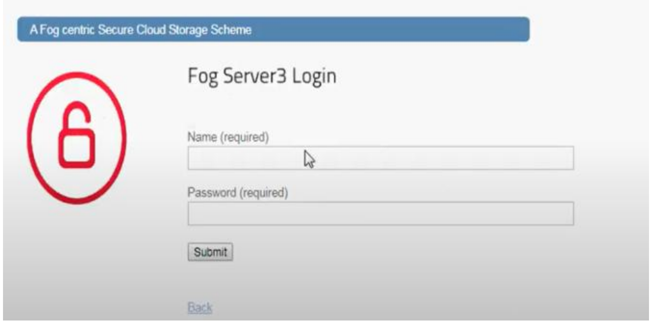

A Fog centric Secure Cloud Storage Scheme

Fog Server2 Login

Name (required)

Password (required)

Fig.8. *FogServer* Login 2

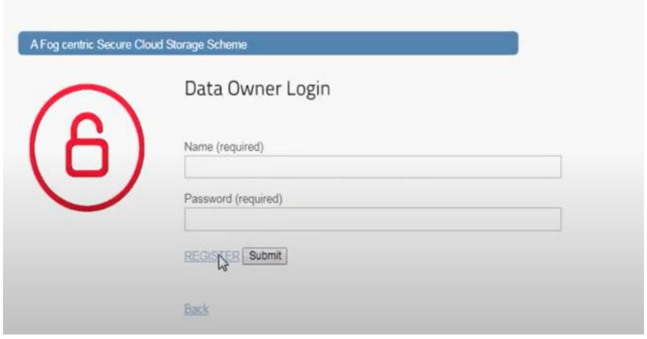

A Fog centric Secure Cloud Storage Scheme

Fog Server3 Login

Name (required)

Password (required)

Fig.9. *FogServer* Login 3

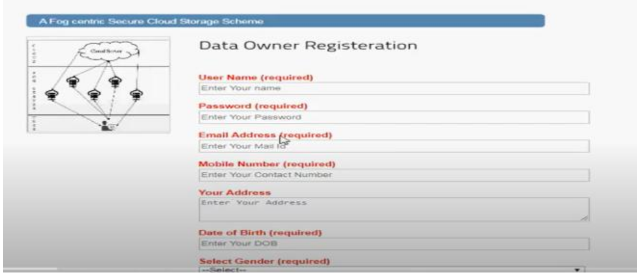

A Fog centric Secure Cloud Storage Scheme

Data Owner Login

Name (required)

Password (required)

Fig.10.Data Owner Login


A Fog centric Secure Cloud Storage Scheme

Data Owner Registeration

User Name (required)
Enter Your name

Password (required)
Enter Your Password

Email Address (required)
Enter Your Mail Id

Mobile Number (required)
Enter Your Contact Number

Your Address
Enter Your Address

Date of Birth (required)
Enter Your DOB

Select Gender (required)
--Select--

Fig.11.Data Owner Registration

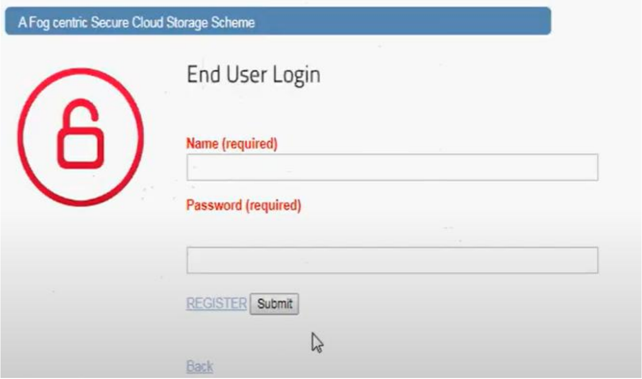


Fig.12.End User Login

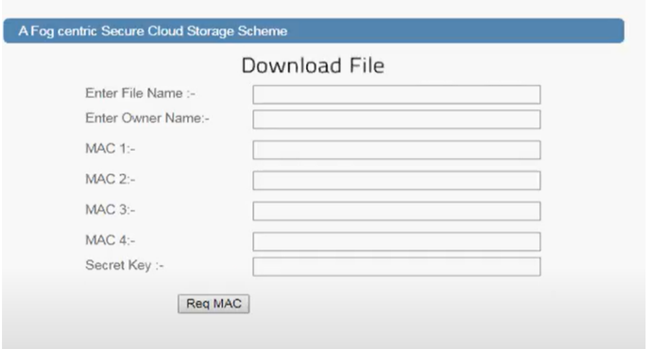


Fig.13.File download

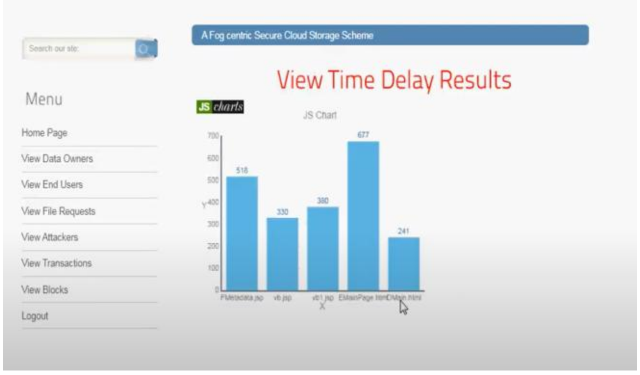


Fig.14.Delay Results

VI. CONCLUSION

The introduction of cloud computing has had several positive effects on the computer industry. As long as users don't send their private information to a cloud storage server, a storage service is great. After the user's data is offloaded to the cloud, the cloud server has complete access to and control over that data. User data may be read or browsed. Data may also be irreversibly harmed by cloud hardware or software failures, and it is susceptible to multiple cyberattacks. A secure cloud storage solution that is reliable against cyber attacks pairs with a fog-based three-tier architecture. This article suggests a method that preprocesses data on a reliable fog server before sending it, in twisted form, to a number of cloud servers. As a preventative precaution, this study combines don, CRH, and BV. By breaking the record up into fixed-length chunks and concatenating them, Xor Combination gets it ready for swap. The suggested system does not depend on encryption technology since it may be broken and has computational cost. Block management chooses which mixed blocks are offloaded to which cloud server, ensuring that no one cloud obtains the whole original data set or even only a portion of it. Meanwhile, or Combination together with Blockock Finally, CRH is capable of detecting any modifications. In contrast to the prior technique, the suggested scheme first twists the data using Xor Combination before dumping it to the cloud, ensuring that the short text fragment never reaches the mat's cloud servers. Similar to this, Xor Combination improves data recovery, while CRH nearly makes integrity tests simpler. Security research demonstrates that it is theoretically challenging to retrieve the plaintext from combined. Every negative identification. Numerous comparison trials demonstrate that its performance is superior than that of earlier methods. The following might be used to describe upcoming work in this area:

1. To increase the effectiveness of cloud storage services based on fog.

2. Increasing the security of fog servers for cloud computing infrastructure that is fog-centric.

3. To enable cloud servers to compute secret data without disclosing its contents.

REFERENCES

1. P. Mell and T. Grance, "The NIST definition of cloud computing," Communications of the ACM, vol. 53, no. 6, p. 50, 2010. [CrossRef]
2. X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," Future generation computer systems, 2017.
3. Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya, "Context-aware collect data with energy efficient in Cyber–physical cloud systems," Future Generation Computer Systems, 2017.
4. J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (SDN) and cloud computing environments," in Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 2969-2974: IEEE. [CrossRef]
5. B. Martini and K.-K. R. Choo, "Distributed filesystem forensics: XtreemFS as a case study," Digital Investigation, vol. 11, no. 4, pp. 295-313, 2014. [CrossRef]
6. N. D. W. Cahyani, B. Martini, K. K. R. Choo, and A. Al-Azhar, "Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study," Concurrency and Computation: Practice and Experience, vol. 29, no. 14, 2017. [CrossRef]
7. J. Fu, Y. Liu, H.-C. Chao, B. Bhargava, and Z. J. I. T. o. I. I. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," 2018.
8. C. F. Tassone, B. Martini, and K. K. R. Choo, "Visualizing digital forensic datasets: a proof of concept," Journal of forensic sciences, vol. 62, no. 5, pp. 1197-1204, 2017. [CrossRef]
9. C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, no. 2, pp. 152-163, 2013. [CrossRef]
10. D. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix," Future Generation Computer Systems, vol. 78, pp. 558-567, 2018. [CrossRef]

AUTHORS PROFILE

K. Anuhya, Received B.Tech degree in Computer science and engineering from CMR Engineering College, Hyderabad and pursuing M.Tech in Computer science and engineering from CMR Engineering College, Hyderabad. Her area of research interest is Cloud Computing.

Dr. Gautam Kumar, working as Professor at CMR Engineering College, Medchal, Hyderabad, India and having more than 5+ years of experience in Teaching Field. His Research area includes Cyber Security, Blockchain, Network Security. He published about more than 10 Papers in various National and International Journals.

Mr. Mrutyunjaya S. Yalawar, working as Assistant Professor at CMR Engineering College, Medchal, Hyderabad, India and having more than 3 years of experience in IT-Industries as Software Developer and more than 6 years of Experience in Teaching Field. His Research area includes Artificial Intelligence, Machine Learning, NLP, Cyber Security, Blockchain. He published about more than 15 Papers in various National and International Journals.