ENHANCED AUDITING MECHANISM FOR SECURE AND EFFICIENT DATA STORAGE IN FOG-TO-CLOUD COMPUTING ARCHITECTURES

Kotturi Raju
Scholar,Department of MCA
Vaageswari College of Engineering-Karimnagar

P. Sathish
Assistant Professor,Department of MCA
Vaageswari College of Engineering-Karimnagar

Dr.V.Bapuji
Professor & Head,Department of MCA
Vaageswari College of Engineering-Karimnagar

ABSTRACT: With the increasing proliferation of the Internet of Things, fog-to-cloud computing has emerged as a new and innovative technology. In addition to the cloud service provider, fog-to-cloud computing makes use of mobile sinks and fog nodes. Fog-to-cloud storage integrity auditing differs from traditional cloud storage. Tian and others are developing a public auditing system that uses fog-to-cloud computing. Their solution is inefficient since it employs tough public key cryptography techniques such as proof of knowledge and bilinear mapping. MAC and HMAC, two well-known private key encryption algorithms, are used in this study to create a more efficient and general audit system. I present our auditing solution using MAC and HMAC. The experiment and theoretical analysis demonstrate that our technique reduces communication and processing costs.

Keywords: **Fog-to-cloud computing, Cloud storage, Internet of Things, Cloud service providers (CSPs).**

1. INTRODUCTION

Bonomi et al. (2012) created fog computing, which has been widely used in industrial applications using IoT devices. Fog computing nodes provide fundamental compute, storage, and resources for data preparation and transmission between IoT devices and clouds. For data storage in large-scale applications with limited resources, fog-to-cloud computing may be an appealing solution.

Fog-to-cloud computing must also solve certain fundamental issues that have arisen in traditional cloud computing, such as how to maintain data integrity in cloud service providers (CSPs). An explanation follows.

Some CSPs may attempt to conceal the loss or distortion of vital fog node or IoT device data due to internal or external attacks. Thus, fog-to-cloud computing auditing tools for secure data storage are equally as critical as traditional cloud computing.

In recent years, numerous public and private auditing solutions have been provided for traditional cloud storag, but none are directly applicable to fog-to-cloud computing,. First, because different devices generate different IOT data, consumers (or data owners) should not obtain this data first and construct appropriate authenticators before outsourcing. Second, and more significantly, present auditing systems do not include fog computing nodes, which are required for fog-to-cloud computing. Fog computing nodes quickly analyze and transmit enormous amounts of IoT data. To assure data accuracy in fog-to-cloud computing, new auditing techniques are required. Tian et al. started this and attempted to close the gap in their most recent study. They employed tag-transforming and bilinear mapping to create a public auditing system that protects privacy. They put their technique through rigorous testing and theoretical analysis.

Public auditing schemes typically assign the duty of ensuring user data accuracy to another approved third-party auditor (TPA) with greater computational capacity and auditing experience. Public auditing systems are less effective than private ones. According to Zhang et al., public auditing methods take hundreds or thousands of times longer to outsource, prove, and validate the same data set than private schemes. In some efficiency-oriented scenarios, such as resource-constrained mobile sinks in fog-to-cloud computing, the private auditing method may be preferable. As a result, fog-to-cloud computing private auditing mechanisms must be created.

This work seeks to move in this direction. In particular, I suggest a new auditing system based on private authentication methods such as HMAC schemes, and MAC, which are critical cryptographic primitives. The HMAC strategy verifies CSP data blocks, whereas the MAC method sends data between mobile sinks and fog nodes. TPA is incompatible with this paradigm since both MAC and HMAC parties require a common private key to create or validate tags.

I also used Agrawal and Boneh's successful HMAC methodology and the hash-based MAC method to create the system.

Finally, i evaluated my approach's efficancy and compare it to Tian et al. and two equivalent traditional cloud auditing methodologies described in. The experiment revealed that our system surpassed Tian et al. in terms of computing efficiency and communication expenses. Because of its fog-to-cloud adaptability, our technique predates.

2. LITERATURE SURVEY

Jues and Kaliski's proof of retrievability (PoR) was among the first to address cloud data integrity. PoR can verify data integrity by spot-checking data blocks and applying error-correcting code. This technique can only handle a certain number of verifications. At the same time, Ateniese et al. created RSA-homomorphic authenticators based on PDP that enable public auditing and endless challenges.

Numerous studies have been conducted on communication efficiency.

PDP system dynamic update has been studied in various studies, and. To allow for data dynamics, public auditing systems frequently incorporate several authenticated data formats. In 2011, Wang et al. introduced Merkle-hash-tree public auditing for dynamic data. Zhu et al. introduced an index hash table for data dynamics. Tian et al. (2017) proposed a two-dimensional dynamic hash table for public audits and data updates. Shen et al. created another structure the same year to collect dynamic data. Contains a doubly linked information table and a location array. Few common cloud storage solutions can be applied immediately to fog-to-cloud IoT data storage verification for efficiency and security.

There are two major causes. Fog-to-cloud scenarios generate data from a variety of IoT devices rather than data owners. In a fog-to-cloud scenario, fog nodes play critical roles in processing and communication. They are overlooked in traditional cloud storage. In their recent articles, Tian et al. and Kashif and Mohammed ddressed this issue in public auditing using various approaches. Neither study examines improved private key auditing options. Wu et al.recently presented a fog computing-enabled cognitive network function virtualization technique for an information-centric future Internet, as well as a forwarding communication scheme between fog nodes and future Internet nodes.

J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, ‘‘Charm: A framework for rapidly prototyping cryptosystems,’’ J. Cryptogr. Eng., vol. 3, no. 2, pp. 111–128, Jun. 2013. Charm, an extendable framework, facilitates cryptosystem prototyping. Charm includes a vast library of reusable code, infrastructure for interactive protocols, and modular cryptographic building blocks for developing new protocols. Our framework also includes specific tools for cryptosystem interoperability. Charm was used to implement more than 40 cryptographic methods, some of which had not previously been evaluated. This page discusses our modular architecture, which includes a benchmarking module for comparing Charm primitives with other C implementations. I illustrated that our techniques frequently cut code size by an order of magnitude while maintaining reasonable performance consequences. Finally, the Charm framework is accessible to scientists, and I have a sizable and active user base.

S. Agrawal and D. Boneh, ‘‘Homomorphic MACs: MAC-based integrity for network coding,’’ in Applied Cryptography and Network Security, (Lecture Notes in Computer Science), vol. 5536. Berlin, Germany: Springer, 2009, pp. 292–305. Network coding has been proven to increase network capacity and resilience. Standard MACs and checksums are ineffective for verifying data integrity because intermediary nodes change packets during transport. In pollution attacks, a single rogue node bombards the network with malicious packets, making it difficult for the recipient to decipher them. Signature systems have been tried to prevent online per-packet integrity attacks, however they are too slow.

I introduced a homomorphic MAC for network-coded data integrity checks. I

created a homomorphic MAC to replace HMACs in network coding systems.
G. Ateniese, R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, 2007, pp. 598 609. A client storing data on an untrusted server can use our proven data possession (PDP) notion to verify that the server owns the data without having to retrieve it. The method provides probabilistic possession proofs by randomly picking server blocks, which reduces I/O costs. The customer collects data to verify evidence. To decrease network transmission, the challenge/response protocol delivers very minimal, consistent data. Thus, the PDP paradigm for remote data checking can handle enormous data sets in dispersed storage systems. Our two provably safe PDP systems outperform schemes with lower guarantees. Specifically, server overhead is low or constant independent of data size. According to our implementation experiments, PDP is feasible, with speed limited by disk I/O rather than cryptographic computation.

G. Ateniese, S. Kamara, and J. Katz, ‘‘Proofs storage from homomorphic identification protocols,’’ in Advances in Cryptology. Berlin, Germany: Springer, 2009, pp. 319–333. Proofs of storage (PoS) are interactive protocols that allow clients to validate the storage of files on a server. A previous research demonstrated that every homomorphic linear authenticator can prove storage. These signature/message authentication systems can generate any linear combination of messages by homomorphically combining their "tags." Our method allows any identification mechanism that meets homomorphic criteria to generate public-key HLAs. then I demonstrate how to convert any public-key HLA into a publicly verifiable proof of stake, with unbounded verifications and communication cost independent of file size. I demonstrate how to apply our modifications to Shoup's identification protocol to build the first factoring-based unbounded-use PoS in the random oracle paradigm.

A. F. Barsoum and M. A. Hasan, ‘‘Provable multicopy dynamic data possession in cloud computing systems,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015. Many businesses are outsourcing data to faraway cloud service providers. Customers can use the CSP's storage infrastructure to store and retrieve virtually infinite data for GB per month. Some customers may require data replication over numerous servers in different data centers for scalability, availability, and durability. Customers pay more for CSP storage of extra copies. Clients must ensure that the CSP maintains all data copies as specified in the service agreement, and that these copies correspond to the most recent client modifications. The map-based proven multicopy dynamic data possession (MB-PMDDP) method I propose in this study demonstrates to clients that the CSP is not deceiving them by keeping fewer copies; 2) it facilitates dynamic data outsourcing by supporting block-level operations such as block modification, insertion, deletion, and append; and 3) it allows authorized users to easily access the file c. compared the proposed MB-PMDDP approach to a reference model built by expanding the database of verified dynamic single-copy systems. Experimental evidence supports theoretical analysis on a for-profit cloud platform. I also demonstrate how to detect corrupted copies by making modest modifications to the provided technique and protecting against collaborating servers.

F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ‘‘Fog computing and its role in the Internet of Things,’’ in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput., New York, NY, USA, 2012, pp. 13–16. Fog computing extends Cloud Computing to the network edge, enabling new services and applications. The fog features low latency, position awareness, wide geographic dispersion, mobility, a large number of nodes, wireless access, streaming and real-time applications, and heterogeneity. I believe that the Fog is the finest platform for Smart Cities, Smart Grids, Connected Vehicles, and Wireless Sensors and Actuators Networks (WSANs) because to its features.

3. EXISTING SYSTEM

The study was conducted by Kaliski and Jues. Spot checks on data blocks can be used to demonstrate that the data is correct and reliable, along with code that corrects errors in Proof of Retrievability (PoR). Having said that, this method has a limited number of verification operations that it can perform. Atniese et al. developed RSA homomorphic authenticators based on proveable data possession (PDP). These can support both public auditing and an infinite number of challenges simultaneously.

Several subsequent studies investigated methods for improving communication efficiency. Several other studies have examined the dynamic updating of PDP schemes. Different types of authenticated data structures are frequently used in public auditing schemes to facilitate data movement. Wang et al. introduced Merkle-hash tree-based public auditing for dynamic data in 2011. To make data dynamic, Zhu et al. invented a new type of data structure known as an index hash table. Tian et al. (2017) developed a new type of data structure known as a dynamic hash table, which can be used for both public auditing and real-time data updates. That same year, Shen et al. developed a new structure for obtaining dynamic data. The structure consists of a doubly linked information table and an array of locations.

Some good ideas have been proposed for traditional cloud storage, but few of them can be directly applied to ensure that data storage in fog-to-cloud-based IoT scenarios is efficient and secure. Two major factors are to blame. When data is transferred from fog to cloud, the IoT devices that created it typically own it. When fog transforms into cloud, new entities emerge, such as fog nodes, which are critical for processing and transmitting data. However, traditional cloud storage does not take them into account.

Tian et al. and Kashif and Mohammed addressed this gap in public auditing several months ago using different methods. However, neither paper discusses the improved private key auditing schemes.

4. PROPOSED SYSTEM

The proposed system aims to move in this direction. I proposed a new auditing approach that employs private authentication methods such as the homomorphic MAC (HMAC) schemes and the message authentication code (MAC). Both of these are fundamental cryptographic concepts with significant implications for security. The MAC method is used to send data between mobile sinks and fog nodes, whereas the HMAC scheme ensures that data blocks stored in CSP are correct. This model is not suitable for adding TPA because everyone involved in MAC or HMAC operations must share a private key in order to create or verify tags. I also demonstrate how to use the system by implementing the effective HMAC scheme developed by Agrawal and Boneh in nd the hash-based MAC scheme developed in.

Advantages:

How to Protect Your Data. Keeping attacks at bay while updating on the fly. Improved data auditing and recovery methods allow for more secure remote data transmission and reception.

SYSTEM ARCHITECTURE

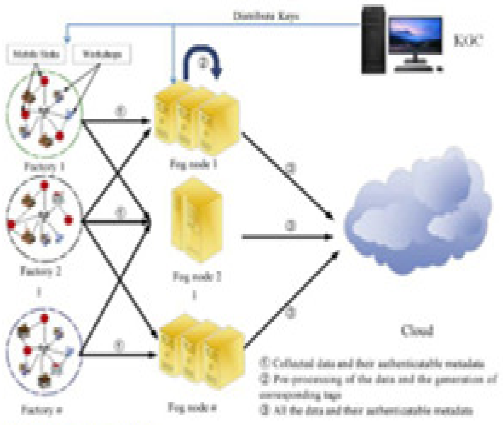

Distribute Keys
KGC
Mobile Sinks
Workshops
②
①
①
①
Factory 1
Factory 2
Factory n
Fog node 1
Fog node 2
Fog node n
③
③
③
Cloud
① Collected data and their authenticatable metadata
② Pre-processing of the data and the generation of corresponding tags
③ All the data and their authenticatable metadata

FIGURE 1. System model.

5. IMPLEMENTATION

SENDER (OWNER):

Before using this module, the sender must complete the registration process and obtain permission. After receiving permission to upload a file, the sender can use a trapdoor to do so. After that, they will be given the option of changing, deleting, checking, or retrieving the uploaded file.

CSP:

The owner (Sender) and user (Receiver) will be able to access this module via the CSP module. In addition, you can see both your uploaded file and the attackers' files in the cloud. You can view the decrypted files, as well as the transaction details and secret keys associated with them.

RECEIVER (USER):

This module requires users to sign up, verify their identity, search for files with keywords, and request a secret key. Once authorization and decryption permissions have been granted, the user can retrieve the desired file from the cloud.

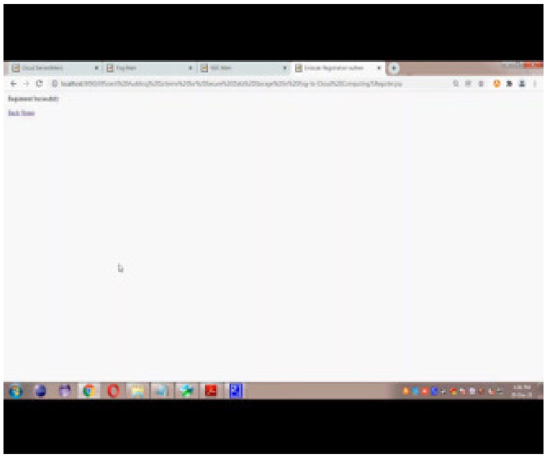
FOG:

Accesses and decrypts user permission requests, grants them, and displays the transaction history and associated metadata.

KGC:

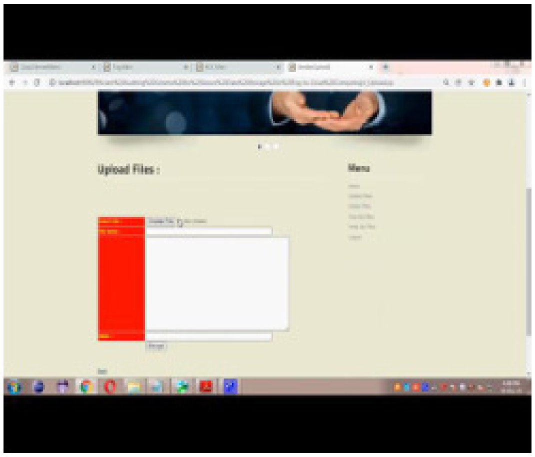
In this module, the private key generator is used to obtain the secret key. The key is separated into two parts, pkey1 and pkey2. This generated key is unique to each file and can be used by multiple users to access all generated secret keys and associated transactions.

6. OUTPUT RESULTS

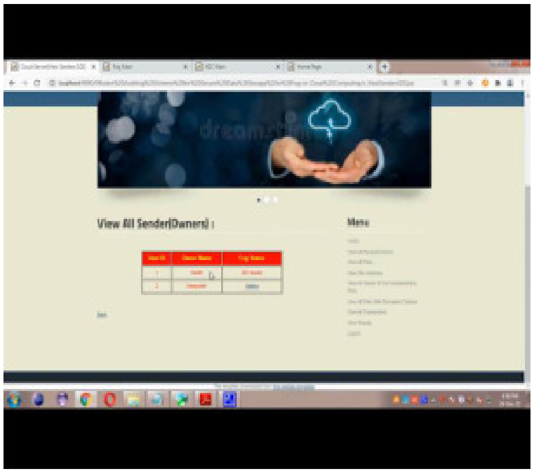


Registered Successfully!

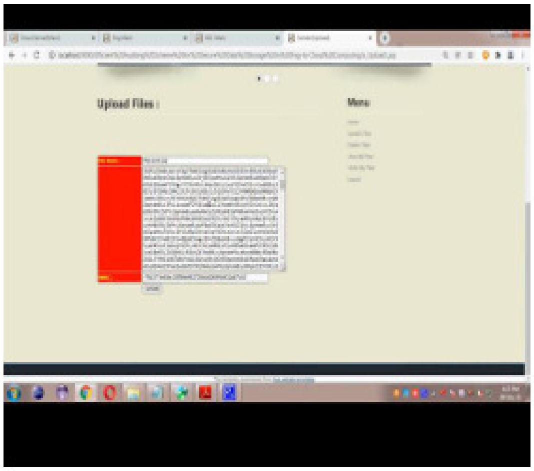
Back Home



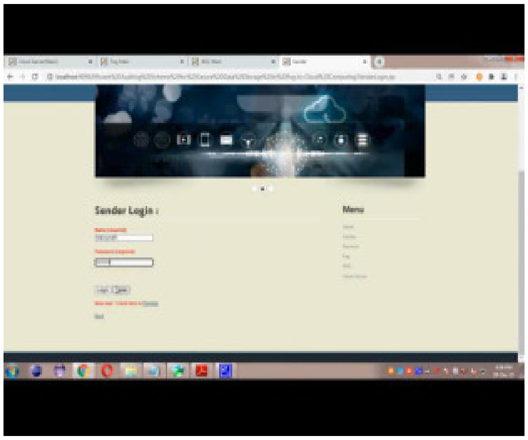
Upload Files :



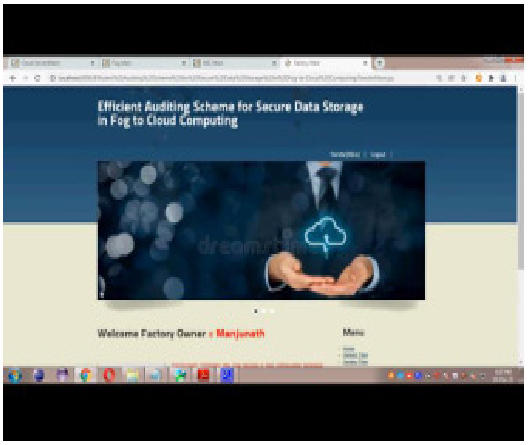
View All Sender(Owners) :



Upload Files :

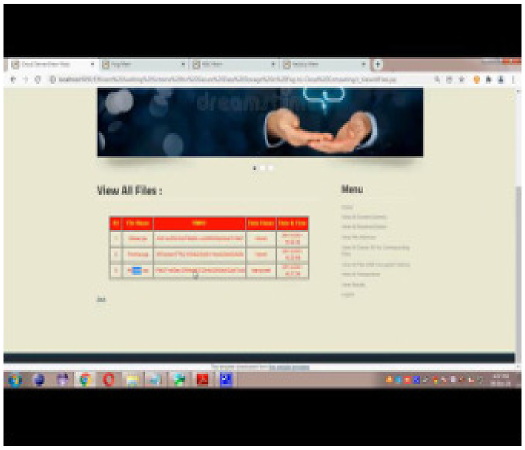


Sender Login :



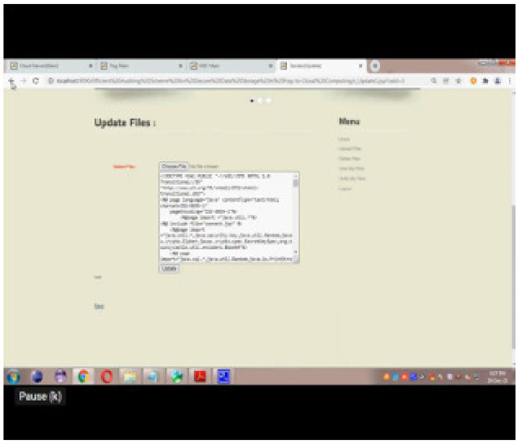
Efficient Auditing Scheme for Secure Data Storage in Fog to Cloud Computing

Welcome Factory Owner : Manjunath



View All Files :

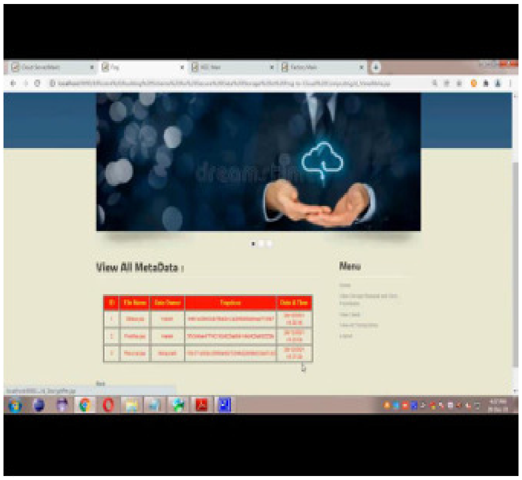
Menu



Update Files :

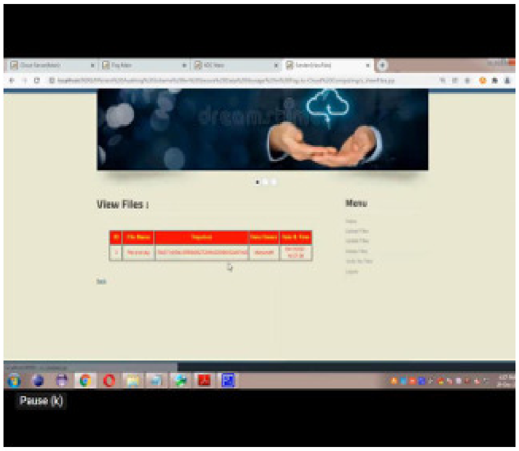
Menu

Pause (k)



View All MetaData :

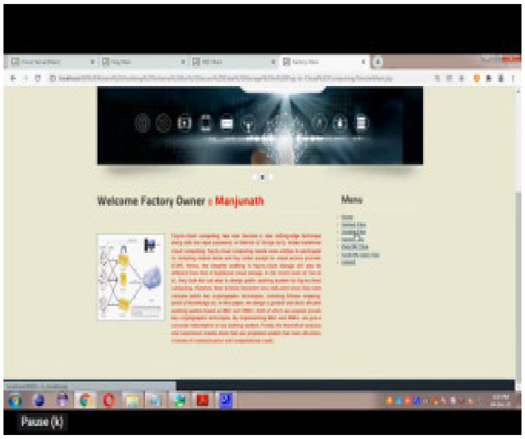
Menu



View Files :

Menu

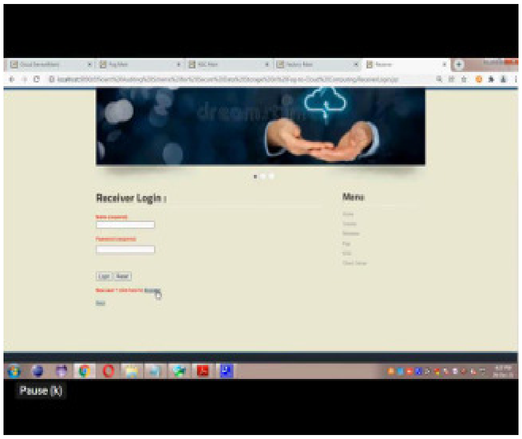
Pause (k)



Welcome Factory Owner : Manjunath

Menu

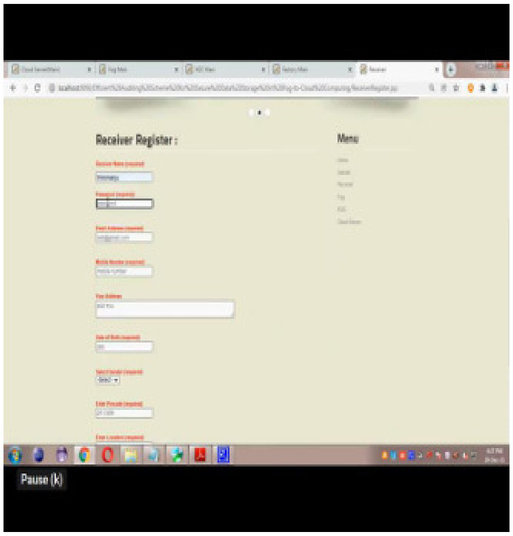
Pause (k)



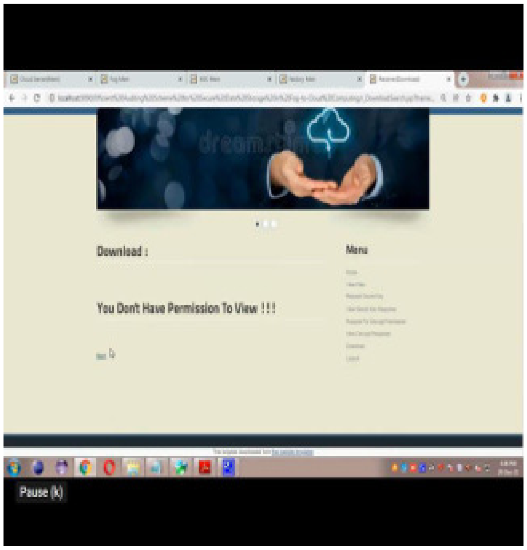
Receiver Login :

Menu

Pause (k)

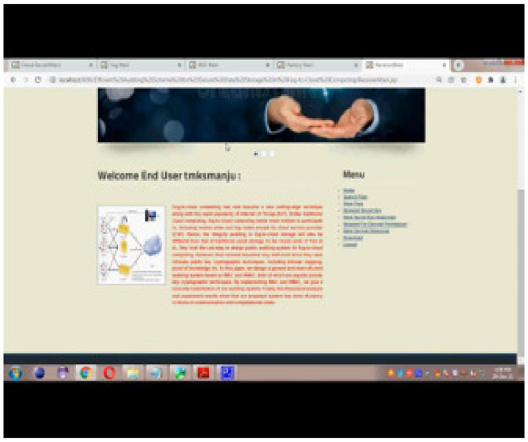


Receiver Register :

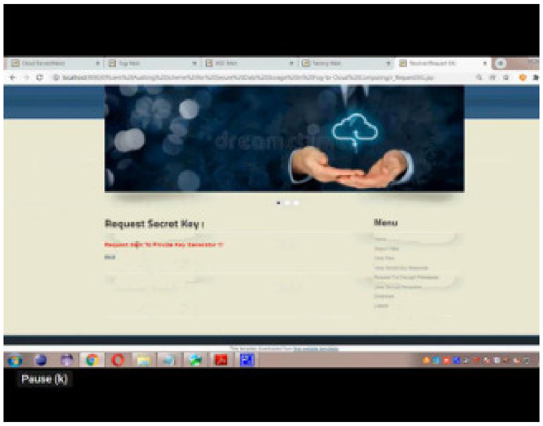


Download :

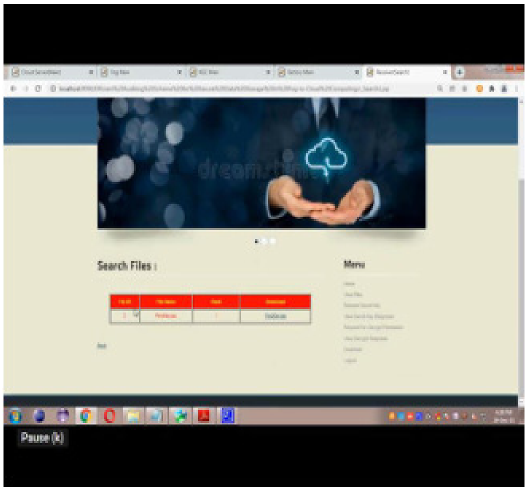
You Don't Have Permission To View !!!



Welcome End User tmksmanju :

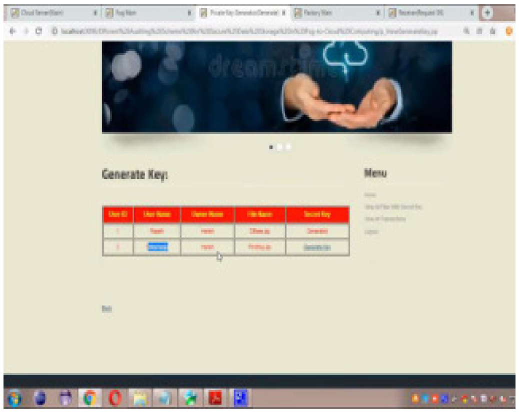


Request Secret Key :



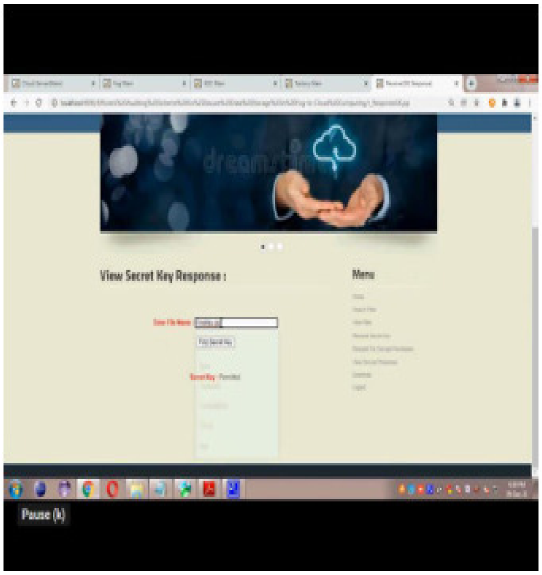
Search Files :

File ID	File Name	Rank	Download
1	[illegible]	1	Download



Generate Key:

User ID	User Name	Owner Name	File Name	Secret Key
1	[illegible]	[illegible]	[illegible]	Generated
2	[illegible]	[illegible]	[illegible]	[illegible]



8. CONCLUSION

This paper proposes an effective auditing system for fog-to-cloud computing. In terms of communication and computing efficiency, our system outperforms the one proposed by Tian et al., despite not having been publicly tested. The simulation results indicate that the computations were completed quickly. If you want to store data safely in fog-to-cloud computing, I believe our proposed solution is an excellent option.

9.REFERENCES

1. V. Subrahmanian and S. Kumar, ``Predicting human behavior: The next frontiers," Science, vol. 355, no. 6324, p. 489, 2017.
2. H. Lauw, J. C. Shafer, R. Agrawal, and A. Ntoulas, ``Homophily in the digital world: A LiveJournal case study," IEEE Internet Comput., vol. 14, no. 2, pp. 15_23, Mar./Apr. 2010.
   Sathish Polu and Dr. V. Bapuji, "Distributed Denial of Service (DDOS) Attack Detection in Cloud Environments Using Machine Learning Algorithms", International Journal of Innovative Research in Technology, (IJIRT), Volume 9, Issue7, ISSN:2349-6002.December 2022, (UGC CARE LIST – I). https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=6hPSwVgAAAAJ&citation_for_view=6hPSwVgAAAAJ:UebtZRa9Y70C
3. M. A. Al-Garadi, K. D. Varathan, and S. D. Ravana, ``Cybercrime detection n online communications: The experimental case of cyberbullying detection in the Twitter network," Comput. Hum. Behav., vol. 63, pp. 433_443, Oct. 2016.
4. L. Phillips, C. Dowling, K. Shaffer, N. Hodas, and S. Volkova, ``Using social media to predict the future: A systematic literature review," 2017, arXiv:1706.06134. [Online].
5. Sathish Polu and Dr. V. Bapuji," "Mitigating Ddos Attacks in Cloud Computing Using Machine Learning Algorithms", The Brazilian Journal of Development ISSN 2525-8761, published by Brazilian Journals and Publishing LTDA. (CNPJ 32.432.868/0001-57) Vol.No.10, Pages:340-354January2024.
6. H. Quan, J. Wu, and Y. Shi, ``Online social networks & social network services: A technical survey," in Pervasive Communication Handbook. Boca Raton, FL, USA: CRC Press, 2011, p. 4.
7. J. K. Peterson and J. Densley, ``Is social media a gang? Toward a selection, facilitation, or enhancement explanation of cyber violence," Aggression Violent Behav., 2016.
8. BBC. (2012). Huge Rise in Social Media.
9. Sathish Polu and Dr. V. Bapuji. "Analysis of DDOS Attack Detection in Cloud Computing Using Machine

Learning Algorithm”, Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages:2410-2418, ISSN:1001-4055, December2023. https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=CC4GukQAAAAJ&citation_for_view=CC4GukQAAAAJ:RYcK_YlVTxYC

10. P. A.Watters and N. Phair, ``Detecting illicit drugs on social media using automated social media intelligence analysis (ASMIA)," in Cyberspace Safety and Security. Berlin, Germany: Springer, 2012, pp. 66_76.
11. M. Fire, R. Goldschmidt, and Y. Elovici, ``Online social networks: Threats and solutions," IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 2019_2036, 4th Quart., 2014.
12. N. M. Shekokar and K. B. Kansara, ``Security against sybil attack in social network," in Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES), 2016, pp. 1_5.