e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cloud and Fog Environment Using Data Integrity Audit

Shaikh Mohamad[1], Jatoth Aravind[2], Mohammad Anas[3], Kavili Sai krishna[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology,Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad,Telangana, India[2,3,4]

ABSTRACT: Cloud-fog computing is a novel computing model that expands the functionality of cloud computing, which provides various services through fog nodes. The issue of traditional data integrity auditing are low data security, slow data processing speed and low communication efficiency. To solve these problems, this paper proposes a data integrity audit scheme based on datablinding. This scheme uses the edge devices in the transmission node to establish a fog computing layer between the cloud service provider and the data owner to reduce transmission delay. The subordinate distribution relationship and weight between fog nodes dynamically allocate the optimalpath and transmit the data to reduce transmission delay. At the same time, a blind factor is added to the integrity audit in the evidence generation process to avoid data leakage. This paper gives a security model and security proof based on computational Diffie-Hellman (CDH) assumptions. The experimental results show that the fog computing layer and blind factor are introduced into the dataintegrity audit process, which can reduce the data communication delay effectively and improve thesecurity of data audit.

KEYWORDS: Cloud-Fog Computing, Data Integrity Audit, Data Blinding, Fog Nodes, Edge Devices

I. INTRODUCTION

In recent years, as the abundance of information has grown, the storage and computing requirementson mobile phones, computers, and other terminal devices have increased. To reduce the storage pressure on terminal devices, some users store their data in the cloud. However, some cloud serviceproviders could delete some infrequently used data to reduce server overhead. Deleted data may notbe retrieved, resulting in cloud data loss. As users upload data, the data is stored on the cloud serverinstead of the local device. Remotely checking the integrity of the data uploaded by users has becomean urgent problem.

In response to the above problems, the concept of Remote Data Possession Checking (RDPC) is proposed, which includes proof of retrievability (POR) and provable data procession (PDP). However,from the perspective of data audit, it can be divided into private and public audits. The auditor of theprivate audit is the data owner, while the auditor of the public audit can be any authorized third-party audit. Dueto the higher flexibility of public auditing methods, most of them will choose public auditing.

As the internet has found its way into people's lives, cloud computing enjoys rising popularity amongindividuals of all stripes. More and more users store their data in the cloud for easy use anytime, anywhere. However, in the traditional cloud storage model, the cloud service provider needs to establish a connection with each user, which invisibly increases the load pressure on the cloud serviceprovider. Therefore, how to reduce the computing and load pressure of cloud service providers hasbecome an urgent problem to be solved.

In the context of data integrity audits, cloud servers are usually far away from the user end. Long- distance data transmission would occupy network bandwidth and increase transmission delay. To solve this problem, the concept of fog computing is proposed. Fog computing expands the concept ofcloud computing. Compared with cloud computing, it is closer to the data owner. In data transmission,the fog node layer is added to reduce the delay and bandwidth. Hu et al. proposed a security and privacy protection scheme based on the fog computing framework, which did not consider the datatransmission model in the fog computing framework.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

H. Wang, D. He(2021)With the rapid development of cloud computing, more and more enterpriseswould like to upload and store their data in the public cloud. When the parts of the business of an enterprise are purchased by another enterprise, the corresponding data will be transferred to the acquiring enterprise. For the usual case, how to outsource the computation cost of data transfer to the cloud? How to ensure the remote purchased data integrity? Thus, it is important to study provabledata possession with outsourced data transfer (DT-PDP). In this paper, for the first time, we propose the novel concept: DT- PDP. By taking use of DT-PDP, the following three security requirements can be satisfied: (1) the other un-purchased data security of acquired enterprise can be ensured; (2)the purchased data integrity and privacy can be ensured; (3) the data transferability's computation can be outsourced to the public cloud servers. For the security concept of DT-PDP, we give its motivation, system model and security model. Then, we design a concrete DT-PDP scheme based on the bilinear pairings. At last, we analyze the security, efficiency and flexibility of the concrete DT-PDP scheme. It shows that our scheme is provably secure and efficient.

J. Chang(2021)Network coding offers the potential to increase throughput and improve robustness without any centralized control. Unfortunately, network coding is highly susceptible to "pollution attacks" in which malicious nodes modify packets improperly so as to prevent message recovery atthe recipient(s); such attacks cannot be prevented using standard end-to-end cryptographic authentication because network coding mandates that intermediate nodes modify data packets in transit. Specialized "network coding signatures" addressing this problem have been developed in recent years using homomorphic hashing and homomorphic signatures. We contribute to this area in several ways: We show the first homomorphic signature scheme based on the RSA assumption (in the randomoracle 2 model). We give a homomorphic hashing scheme that is more efficient thanexisting schemes, and whichleads to network coding signatures based on the hardness of factoring (in the standard model). We describe variants of existing schemes that reduce the communication overhead for moderate-size networks, and improve computational efficiency (in some cases quite dramatically – e.g., we achievea 20- fold speedup in signature generation at intermediate nodes).

K. Gu(2020)Fog computing is mainly used to process a large amount of data produced by terminal devices. As fog nodes are the closest acquirers to the terminal devices, the processed data may be tampered with or illegally captured by some malicious nodes while the data is transferred or aggregated. When some applications need to require real-time process with high security, cloud service may sample some data from fog service to check final results. In this paper, we propose a secure data query framework for cloud and fog computing. We use cloud service to check queried data from fog network when fog network provides queried data to users. In the framework, cloud server pre-designates some data aggregation topology trees to fog network, and then fog network may acquire related data from fog nodes according to one of the pre-designated data aggregation trees. Additionally, some fog nodes are assigned as sampled nodes that can feed back related data to cloud server. Based on the security requirements of fog computing, we analyze the security of our proposed framework. Our framework not only guarantees the reliability of required data but also effectively protects data against man-in-the- middle attack, single node attack and collusion attack of malicious users. Also, the experiments show our framework is effective and efficient. With the rapid development of network, cloud computing has become a very important application servicein many other industry fields, such as Internet of Things (IoT). However, more and more terminal devices are connected to IoT, which may produce massive and diverse data every day. So, the modelof cloud computing is difficult to meet the needs of IoT for responding quickly, high mobility, geographical distribution, location awareness, low latency and so on. The Cisco company proposeda new computing concept called as fog computing, which moves computing, storage and other functions of cloud computing from the center to the edge of network where all functions are closerto terminal users.

S. Xu(2020)Related-key attack (RKA) is a kind of side-channel attack considered for kinds of cryptographic primitives, such as public key encryption, digital signature, pseudorandom functionsetc. However, we note that the RKA-security seems to be not considered for identity-based signature (IBS), which is an important primitive for identity-based cryptography and proposed by Shamir in 1984. In this paper, for the first time, we introduce the RKA security into IBS schemes and try to define the security model for it. More specifically, we consider the RKA occurs in the users' signing key or the master key of the Key-Generation Center (KGC), which derives two kinds of RKA securities for IBS. Meanwhile, we illustrate that the most efficient Schnorr-like IBS scheme proposed by Galindo and Garcia is RKA-insecure by launching a simple RKA. However, a slight modification of it yields a RKA-secure IBS scheme, for which

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

we give the detailed security proof in the random oracle. Finally, the performance analysis shows that the modified scheme is still extremely efficient but has higher security. Digital signature is a fundamental primitive in public key cryptography [18], which ensure the authenticity of the originator of a digital document as wellas the integrity of that document. A signature for some digital document is valid if it can pass the verification test algorithm, which usually needs a verification key sent from the originator as input.Hence, external binding between the verification key and the signing entity is needed. The general way is using certificate from a trusted certification authority.

Existing System

- Most existing tracking and traceability system, which is used by most supply chain networks, has problems with centralized management and data privacy.
- The issue of traditional data integrity auditing are low data security, slow data processing speed and low communication efficiency.
- It's veryconstructed a technology based entirely on symmetric key encryption andeffectively supports block modification, deletion, and append operations.

Disadvantages of existing system:

- Low data processing speed.
- Low communication Efficiency.
- The existing system less security of data audit.

Proposed System

This paper gives a security model and security proof based on computational Diffie-Hellman(CDH) assumptions. This paper proposes a data integrity audit scheme based on the cloud and fog architecture, meanwhile, provides a data transmission model in the cloud and fog network
In this model, the data is transmitted and calculated by fog nodes to find the lowest communicationchannel, thereby reducing communication overhead.

Proposed System Advantages

- High data processing speed.
- It's reduce the data communication delay effectively and improve the security ofdata audit.

System Architecture

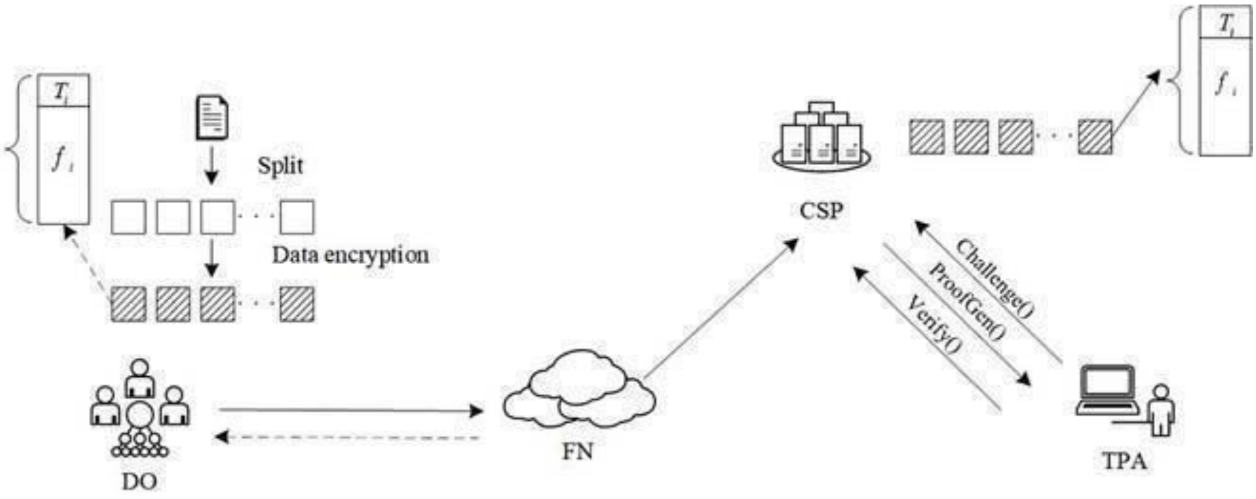


Fig 1.1 System Architecture

In our Project we have a three virtual machines in the project. Admin has a login witha user id and password. Admin have a view a virtual machines. Admin can have a resource manager virtual machines. Admin have a cloud provider information. Admin can also have a user data information of the details. Admin have a backup data.

III. METHODOLOGY

Module Name:

- User Interface Design
- Admin
- User
- Third-Party Auditor (TPA)
- Summarization

1) **User Interface Design**:To connect with server user must give their username and password thenonly they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into theserver. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.
2) **Admin**: Admin has key role in our project, the uploaded file will be getting to the admin module from the user, where he will verify the file and try to send the file to the THREE LAYRED FRAMEWORK (Cloud Server Layer, Fog Layer and Endpoint Layer). Admin will be getting the security alerts about the file present in the servers respectively. Fog computing nodes (FN) are interconnected edge devices with precise computing capabilities, such as gateways, switches and routers
3) **User:** This is the 2nd module of our project where user after successfully registration, will to upload the files in to the server, whenever he is uploading a new file a unique key will be generatedand uploaded file will be splinted in to 3 different parts by using "DCBF model Algorithm". This file will be transferred in to the next phase of the project.
4) **Third-Party Auditor (TPA) or Three-Layered Server Framework (TLS)**: This module will present the whole project scenario, here we will be having '3' servers such as "Local machine" where 1% of the data will be stored, "Fog Server" where 4 percent of the data will be stored, and the remaining 95% of the data will be stored in the "Cloud Sever". In order to protect user's privacy, along with the TLS framework we will also use encryption mechanism in our project. The third- party auditor (TPA) will review the integrity of the outsourced data for the data owner.
5) **Summarization:** In order to solve the problem of privacy protection in cloud storage, we proposea TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server.

Implementation

The Data Blinding for Cloud and Fog (DBCF) model ensures secure data storage and retrieval by leveraging the Computational Diffie-Hellman (CDH) assumption. This model consists of two layers: the cloud service layer, responsible for large-scale data management, and the fog computing layer, which handles localized processing. In this system, users generate their public and private keypairs by initializing the system with a security parameter kkk, which defines a cyclic group GGG ofprime order ppp and a generator ggg. Each user selects a private key xxx randomly from ZpZ_pZpand computes the corresponding public key y=gxmod py = g^x \mod py=gxmodp.

Once the key pair is established, the data owner prepares to upload data securely. The file FFF is divided into multiple blocks BiB_iBi, each of which undergoes a blinding process. Each block BiB_iBi is combined with a random value rir_iri to form the blinded block Bi′=Bi×yrimod pB'_i =B_i \times y^{r_i} \mod pBi′=Bi×yrimodp. Additionally, a tag TiT_iTi is generated for each blockusing a secure hash function, defined as Ti=h(Bi||ri)T_i = h(B_i || r_i)Ti=h(Bi||ri). Finally, the data owner uploads the set of blinded blocks {Bi′}\{B'_i\}{Bi′} and tags {Ti}\{T_i\}{Ti} to the cloud, ensuring that data confidentiality and integrity are preserved throughout the process.

IV. ALGORITHM USED

Existing Algorithm

Computational Diff-Hellman(CDH) Assumption

The CDH assumption is a standard cryptographic hypothesis, and many cryptographic schemes are constructed on this CDH assumption, such as public-key encryption, digital signature, and authentication key exchange. Moreover, complex agreements, such as cloud storage, refusing authentication agreements are also built on this assumption.

Proposed Algorithm

Data Blinding for Cloud and Fog(DBCF) System model

The cloud and fog computing model in the DBCF model can be composed of a cloud service layerand a fog computing layer. This algorithm is used to initialize the system and generates the user's public and private key pair. Enters the security parameter k, and output the corresponding public key and private key. The data owner executes this algorithm to generate the tag set of the uploadedfile, and the data owner uploads the tag set and data block to the cloud accordingly.

Experimental Results

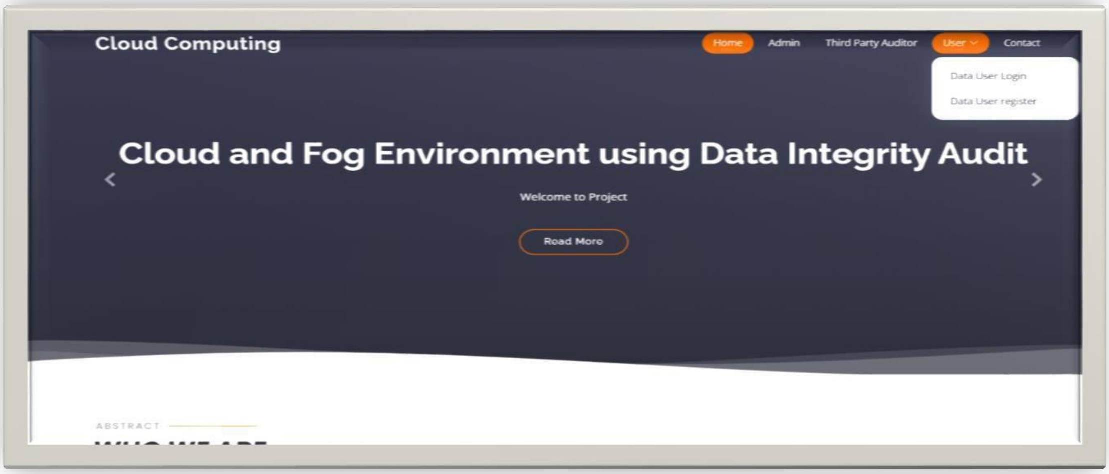
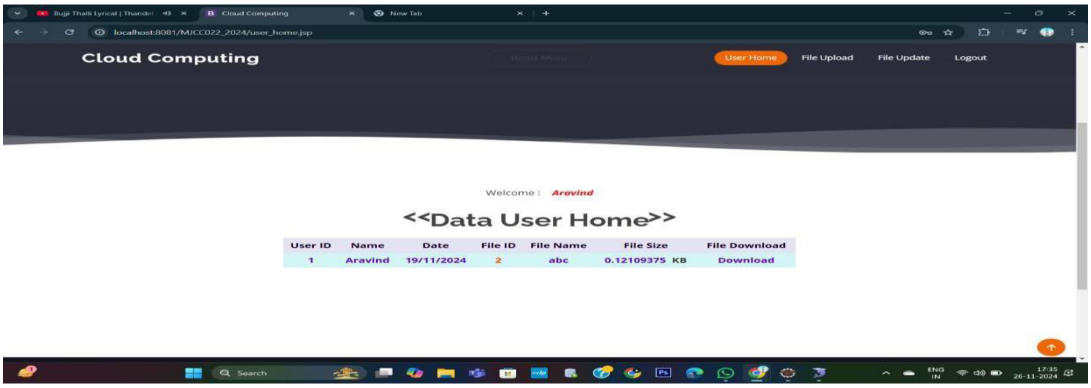


Fig: 2 User Registration Page

- Register with User Name and Password



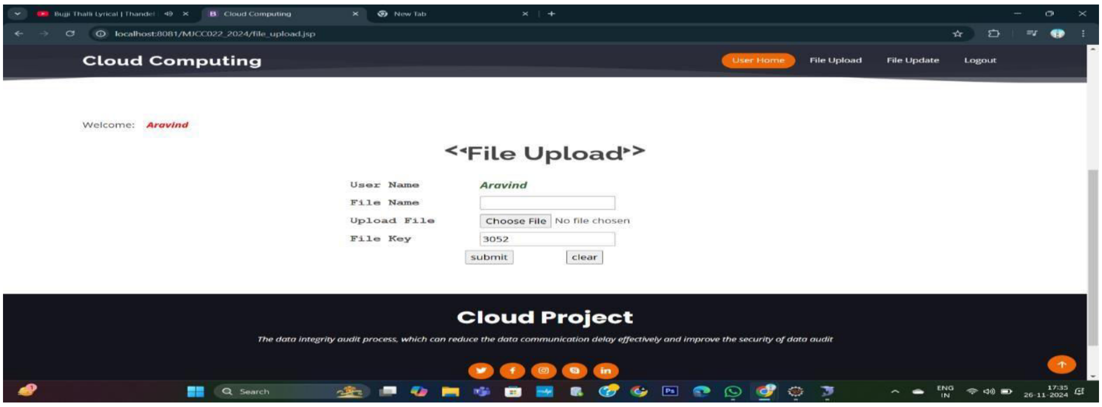
Welcome : *Aravind*

<<Data User Home>>

User ID	Name	Date	File ID	File Name	File Size	File Download
1	Aravind	19/11/2024	2	abc	0.12109375 KB	Download

Fig: 3 User File Viewer Page

- User’s Cannot upload file directly it takes a permission from a cloud provider.



localhost:8081/MJCC022_2024/file_upload.jsp

Cloud Computing

Welcome: Aravind

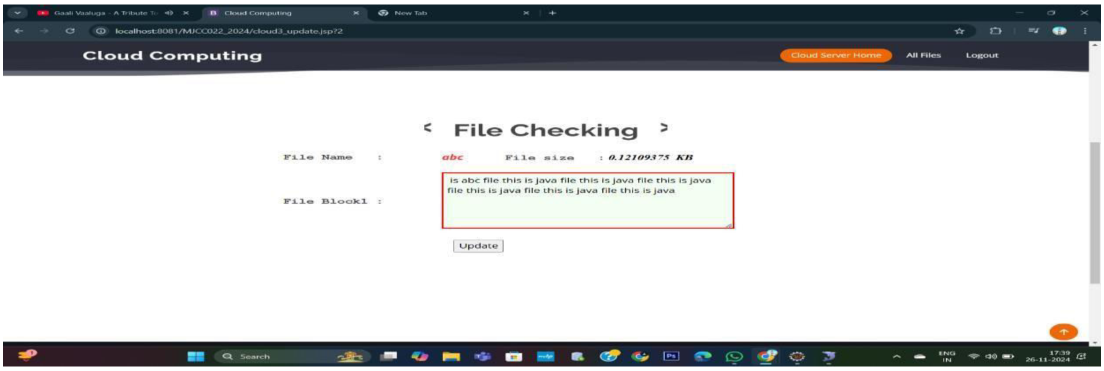
<<File Upload>>

User Name: Aravind
File Name:
Upload File: Choose File No file chosen
File Key: 3052

Cloud Project

The data integrity audit process, which can reduce the data communication delay effectively and improve the security of data audit

Fig: 4 User Data Upload Page



localhost:8081/MJCC022_2024/cloud3_update.jsp?2

Cloud Computing

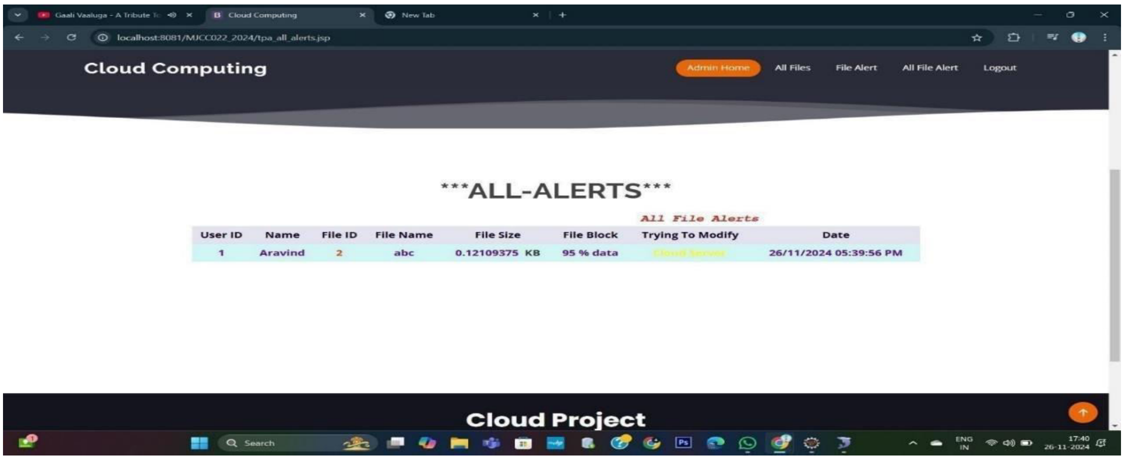
< File Checking >

File Name : abc File size : 0.12109375 KB

File Block1 : is abc file this is java file this is java file this is java file this is java file this is java file this is java

Fig: 5 User Data Upload Page

- TPA cannot have access to modify the data from the Database.



localhost:8081/MJCC022_2024/tpa_all_alerts.jsp

Cloud Computing

ALL-ALERTS

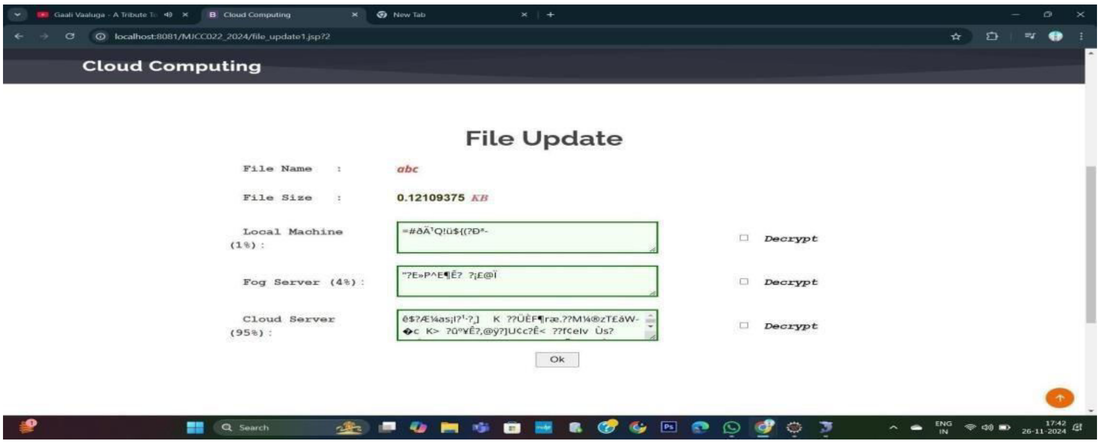
All File Alerts

User ID	Name	File ID	File Name	File Size	File Block	Trying To Modify	Date
1	Aravind	2	abc	0.12109375 KB	95 % data	Cloud Server	26/11/2024 05:39:56 PM

Cloud Project

Fig: 6 Admins Alert Page when TPA will try to modify

- Here Admin can view Alert where the TPA accessed.


Gaali Vaaluga - A Tribute To
Cloud Computing
New Tab
localhost:8081/MJCC022_2024/file_update1.jsp?2
Cloud Computing
Search
ENG
IN
17:42
26-11-2024

File Update

File Name : abc

File Size : 0.12109375 KB

Local Machine (1%) : =#ðÃ'Q!ü${(?Ð³- □ Decrypt

Fog Server (4%) : "?E»P^E¶Ê? ?¡£@Ï □ Decrypt

Cloud Server (95%) : ê$?Æ¼as¡l?'-?,] K ??ÜÈF¶ræ.??M¼®zT£åW- �c K> ?û°¥Ê?,@ÿ?]U¢c?Ê< ??f¢elv Ùs? □ Decrypt

Ok

Fig: 7 User can modify the Data.

- User can modify the data which is stored in cloud.

V. CONCLUSION

This paper proposes a DBCF protocol in the cloud and fog environment. This protocol can ensure data security in the case of data integrity auditing. This scheme introduces a blind factorin the data verification process, and adds random values to each verification, thereby avoidingthe adversary's multiple requests to obtain user information. At the same time, the fog computing layer is established, and the cloud and fog structure is used to change the architectureof the transmission network, which can effectively reduce the communication overhead. In addition, the security model is given and provedto be secure under the random oracle model assumed by CDH.

VI. FUTURE ENHANCEMENT

Finally, the performance analysis shows that this protocol will be more efficient in practical applications. In future work, the architecture model of the fog computing layer can be improved to make it more efficient.

REFERENCES

1. W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges",IEEE Internet Things J., vol. 3, no. 5, pp. 637-646, Oct. 2016.
2. J. Li, Y. Zhang, X. Chen and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", Compute. Secur., vol. 72, pp. 1-12, Jan. 2018.
3. Y. Deswarte, J.-J. Quisquater and A. Saidane, "Remote integrity checking", Proc. Working Conf. Integrity Internal Control Inf. Syst., pp. 1-11, 2003.
4. H. Wang, D. He, A. Fu, Q. Li and Q. Wang, "Provable data possession with outsourceddatatransfer", IEEE Trans. Services Compute., vol. 14, no. 6, pp. 1929-1939, Nov. 2021.
5. C. C. Erway, A. Kupçu and C. Papamanthou, "Dynamic provable data possession", ACM Trans. Inf. Syst. Secur., vol. 17, no. 4, pp. 1-29, 2009.
6. A. Acar, H. Aksu, A. S. Uluagac and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation", ACM Compute. Surv., vol. 51, no. 4, pp. 1-35,2018.
7. H. Wang, L. Feng, Y. Ji, B. Shao and R. Xue, "Toward usable cloud storage auditing revisited", IEEE Syst. J., vol. 16, no. 1, pp. 693-700, Mar. 2022.
8. J. Chang, B. Shao, Y. Ji, M. Xu and R. Xue, "Secure network coding from secure proofof retrievability", Sci. China

Inf. Sci., vol. 64, no. 12, Dec. 2021.

9. A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues", IEEE Internet Compute., vol. 21, no. 2, pp. 34- 42, Mar./Apr. 2017.
10. F. Bonomi, R. Milito, P. Natarajan and J. Zhu, "Fog computing: A platform for Internetof Things and analytics" in Big Data and Internet of Things: A Roadmap for Smart Environments, Cham, Switzerland: Springer, pp. 169-186, 2014.
11. M. Ma, D. He, D. Kumar, K.-K. R. Choo and J. Chen, "Certificateless searchable publickey encryption scheme for industrial Internet of Things", IEEE Trans. Ind. Informant.,vol. 14, no. 2, pp. 759-767, May 2017.
12. J. Zhou, T. Wang, M. Z. A. Bhuiyan and A. Liu, "A hierarchic secure cloud storage scheme based on fog computing", Proc. IEEE 15th Int. Conf. Dependable Auton. Secure Compute. 15th Int. Conf Pervasive Intell. Compute. 3rd Int. Conf. Big Data Intell. Compute. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), pp. 470-477, Nov. 2017.
13. P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things", IEEE Internet Things J., vol. 4, no. 5, pp. 1143-1155,Oct. 2017.
14. H. Yan, J. Li and Y. Zhang, "Remote data checking with a designated verifier in cloudstorage", IEEE Syst. J., vol. 14, no. 2, pp. 1788-1797, Jun. 2020.
15. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, et al., "Provable data possession at untrusted stores", Proc. 14th ACM Conf. Comput.Commun. Secure. (CCS, pp. 598-609, 2007.
16. A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files", Proc. 14th ACM Conf. Compute. Commun. Secur. (CCS), pp. 584-597, 2007.
17. G. Ateniese, R. Di Pietro, L. V. Mancini and G. Tsudik, "Scalable and efficient provable data possession", Proc. 4th Int. Conf. Secure. Privacy Commun. Netw. (SecureComm), pp. 1-10, 2008.
18. H. Shacham and B. Waters, "Compact proofs of retrievability", J. Cryptol., vol. 26, no.3, pp. 442- 483, Jul. 2013.
19. H. Wang, "Proxy provable data possession in public clouds", IEEE Trans. Services Compute., vol. 6, no. 4, pp. 551-559, Oct./Dec. 2013.
20. Y. Ren, J. Xu, J. Wang and J.-U. Kim, "Designated-verifier provable data possession.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com