IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11756

Permitting Cloud Services for Data Mobility and Rapid External Audits

Tharunkumar P [1], K Sharath [2]

Student, Dept. of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Dept. of MCA, Bangalore Institute of Technology, Karnataka, India[2]

Abstract: The availability of public auditing facilitates efficient integrity checks for data stored on cloud servers. This paper reexamines public auditing for encrypted data, emphasizing the management of data dynamics such as modifications, insertions, and deletions. Initially, we identify the component in current auditing methods that most significantly limits data dynamics in terms of cost. Subsequently, we introduce a groundbreaking public auditing technique that delivers significantly faster data dynamics compared to previous methods. Our auditing challenge-response protocol significantly reduces the computational burden on the third-party auditor (TPA), enhancing the speed of verification for auditing results. Effectiveness and security analyses demonstrate that the suggested method minimizes computational costs while ensuring data integrity and privacy against an untrusted cloud.

Keywords: Public Auditing, Cloud Services, Data Mobility, Encrypted Data, Data Dynamics, Third-Party Auditor (TPA)

I. INTRODUCTION

The use of clouds is the utilisation of computer resources (hardware and software) offered as a service across a network (usually the Internet). The term derives from the ubiquitous application of a cloud-shaped logo in system diagrams as a way to represent the complicated architecture it encompasses. Cloud computing entrusts processing, software, and data to distant services. Software and hardware are elements that can be made available over the Internet as part of cloud computing controlled third-party services. These services often give access to sophisticated server network technologies and sophisticated software applications.

Utilizing the cloud aims to apply customary supercomputing, or powerful computing power, typically utilized in consumer-focused operations by research canters and the military to carry out tens of billions of calculations every second such as investing, to deliver personalised knowledge, to provide storage of data, or to power large, complete computer games.

Cloud computing distributes data-processing tasks over networks of large groups of machines, often employing consumer computer technology that is inexpensive and has specialized connectivity. Using low-cost, specialist connection consumer computer technologies interconnected systems. Virtualization methods are frequently utilised to maximise the potential of the internet of things.

The National Institute of Standards and Technology fleshes out five major characteristics of cloud computing.

• On-demand self-service: A customer may supply computing capabilities, like network storage and server time, whenever necessary without involving human contact with the supplier of each service.

• Broad network access: Capabilities are available throughout the network and may be accessed via conventional procedures that encourage the use of heterogeneous thin or thick client platforms (e.g., laptops, mobile phones, and PDAs).

• Resource pooling: Using a multi-tenant approach, the provider's computing resources are combined to service many clients, and different virtual and physical assets are constantly assigned and reallocated based on consumer demand.

Cloud computing can be classified into three service models: IaaS, PaaS, and SaaS. An end-user layer complements these models, reflecting the point of view from the user's perspective. The image below illustrates this model. Say a cloud user runs her own applications, making use of the platform layer.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11756

That would mean she is responsible for their support, maintenance, and security. In contrast, when she utilizes the services of the application layer offered by the cloud service provider, these activities are typically controlled by the provider.

II. LITERATURE SURVEY

Q. Wang**[1]** The most intriguing paradigm change in computing that has occurred in information technology recently is cloud computing. On the other hand, privacy and security have been major hindrances to full adoption. The authors have contributed to this argument with emphasis on some key concerns and further research on measures for a trustworthy open public cloud environment.

Shankar, U.[2] It is difficult to provide good data protection to cloud customers while also enabling complex applications. Researchers investigate Data security as a Service, a new cloud platform architecture that drastically decreases the per-application development work necessary to provide data security while yet allowing for rapid creation and child care.

L. Wei and colleagues [3] Cloud computing arises as a new computing paradigm with the goal of providing cloud customers with dependable, customised, and quality-of-service-guaranteed compute environments. Applications and databases are relocated to huge centralised data centres known as cloud. Because of resource virtualization, global replication and migration, and the physical absence of data and machines in the cloud, stored data and compute results in the cloud may not be adequately managed and fully trusted by cloud users. Most past work on cloud security has focused on storage security as opposed to obtaining compute security into account. In this work, we present Becloud, a first protocol for discouraging privacy cheating and secure computation auditing.

G. Ateniese and colleagues[4] We present a paradigm for proven data possession (PDP), This enables a customer to verify that Without acquiring it, the original data is owned by an untrustworthy server. Utilizing arbitrary block sets selected from the server, the method generates probabilistic proofs of possession while substantially reducing I/O costs. To validate the evidence, the client keeps a consistent quantity of information. The challenge/response protocol sends a modest, consistent quantity of data, reducing network traffic. Thus, for remote data, the PDP model verification can accommodate massive data sets in a globally dispersed storage system.

Tsudik, G. [5] Storage outsourcing is a growing practise that raises a variety of intriguing security concerns, many of Which have already seen an extensive analysis. In contrast, the concept of Provable Data Possession (PDP) is relatively recent in the research literature. The key problem addressed is that of efficiently verifying whether a storage server is reliably storing its client's potentially large outsourced data at regular intervals, efficient, and safe basis. In terms of security and dependability, the storage server is believed to be untrustworthy. (In other words, it may delete hosted material intentionally or inadvertently; it may even relegate it to sluggish or off-line storage.) The client's little computer equipment with low resources exacerbates the situation. This issue has already been addressed.

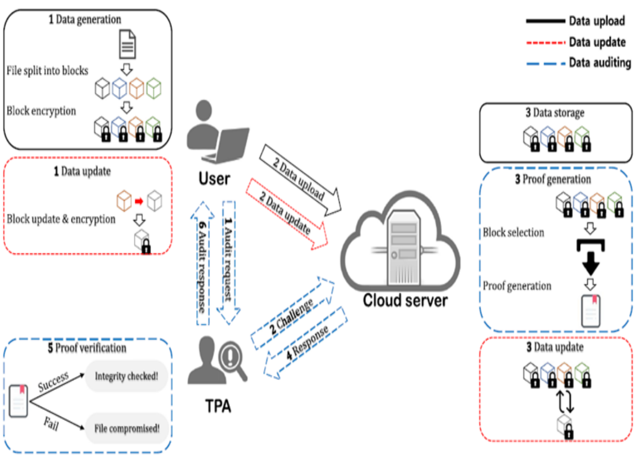

Fig -1: Proposed Architecture

DOI: 10.17148/IARJSET.2024.11756

III. EXISTING MODEL

Ateniese et al. introduced Provable Data Possession (PDP), in which a public verifier may validate a user's cloud-stored data. For outsourced data, PDP employs an RSA-based Homomorphic Linear Authenticator (HLA). Because an HLA may be aggregated, an aggregated HLA that authenticates a linear combination of individual data blocks are calculable. The accuracy of the outsourced data may be verified by the public verifier. without getting the complete data set by using sampling procedures. This technique, however, excludes dynamic processes for outsourced data.

 Another approach known as Proofs of Retrievability (POR) was developed by Juels and Kaliski. The POR method includes unique blocks known as sentinels that are randomly placed in data for detecting purposes. They do, however, limit operations.

Shacham and Waters developed a more robust POR system based on the Boneh-Lynn-Shacham (BLS) signature. It overcomes the POR scheme's restriction in terms of the amount of challenge inquiries and gives proof of security. However, because the cloud cannot discriminate between data blocks and encrypted codewords, it only analyses static data files.

Liu et al. suggested a regenerated code-based technique that allows a user to confirm the accuracy of random sections of outsourced data against corruption. But this approach doesn't handle dynamic data operations.

IV. PROPOSED METHODOLOGY

We provide a unique public auditing approach for encrypted data that allows for extraordinarily rapid data dynamics. We clearly describe the security model and rigorously establish the proposed scheme's security to demonstrate that data integrity and privacy are safeguarded in the presence of an untrusted cloud.

 Our innovative auditing challenge-response technique considerably minimises the TPA's computing cost. In particular, the TPA-side computing cost for verification is a fixed amount of pairings and exponentiations in a cyclic group, whereas previous research required such operations to scale linearly with the quantity of challenged blocks. The proposed technique enables pre-computation capabilities, allowing the TPA to pre-compute all exponentiation operations required for the upcoming phase after sending an auditing request to the cloud.

The suggested approach is compatible with any symmetric-key encryption algorithm, allowing the blocks to be encrypted with any encryption technique that the owner of the data desires.

Because the underlying encryption technique is CPA-secure, data secrecy is guaranteed against the cloud.

We demonstrate that the cloud cannot learn the outsourced data throughout the auditing process and that the cloud cannot manufacture legitimate evidence in response to the TPA's auditing request.

Our innovative auditing challenge-response protocol considerably decreases the TPA's computing cost, enhancing the confirmation speed for audit findings.

V. IMPLEMENTATION

User: In the first module, we create the User component. The user is the entity that has a huge amount of data that has to be kept in the cloud and want to retain data privacy and integrity against the cloud. This module represents the system's end user, who uploads, updates, and audits data. The User module requests data uploads and updates and gets auditing results from the TPA. To protect data integrity and privacy, it communicates with the TPA and Cloud Server modules.

TPA: In this module, we will create a Third-Party Auditor (TPA). The TPA is the entity that validates the integrity of the data saved in the cloud on behalf of the user via a challenge-and-response protocol with the cloud. This module is in charge of auditing the data in the Cloud Server module. It validates the data's integrity and confirms that it has not been tampered with. The TPA uses challenge-response protocols to ensure the data's integrity and produces auditing results for the User module. The suggested method in this project seeks to greatly lower the TPA computation cost in order to boost the verification speed of the auditing findings.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11756

Internet: The Cloud component is being developed in the module. The cloud is an entity offering data storage and computational power for the user's data. This module keeps the encrypted data that the User module uploads. It is in charge of storing and retrieving data, as well as updating data when the User module requests it. For data upload, update, and retrieval actions, the Cloud Server module communicates with the User module. We utilise DriveHQ cloud service provider for real-time cloud storage delivery, whereby the files submitted by will be saved in the DriveHQ server.

Data Upload: This phase is primarily handled by the user. The user creates both public and private settings. Before saving a file on the cloud, he separates it into numerous data chunks. The user must encrypt the data blocks to maintain data confidentiality. To allow the TPA to audit without disclosing the key, the user generates auditing information with homomorphism hash characteristics. Uploading data encrypted in block and auditing information to the cloud is done by the user. He then deletes the auditing information and data blocks from the local storage.

Updated data:
In this step, we presume that the user has already downloaded some things of interest. If he discovers that certain blocks of a file require updating (for example, block modification, insertion, and deletion), he encrypts the modified block and creates new auditing information matching to the new block1. Then he saves it to the cloud.

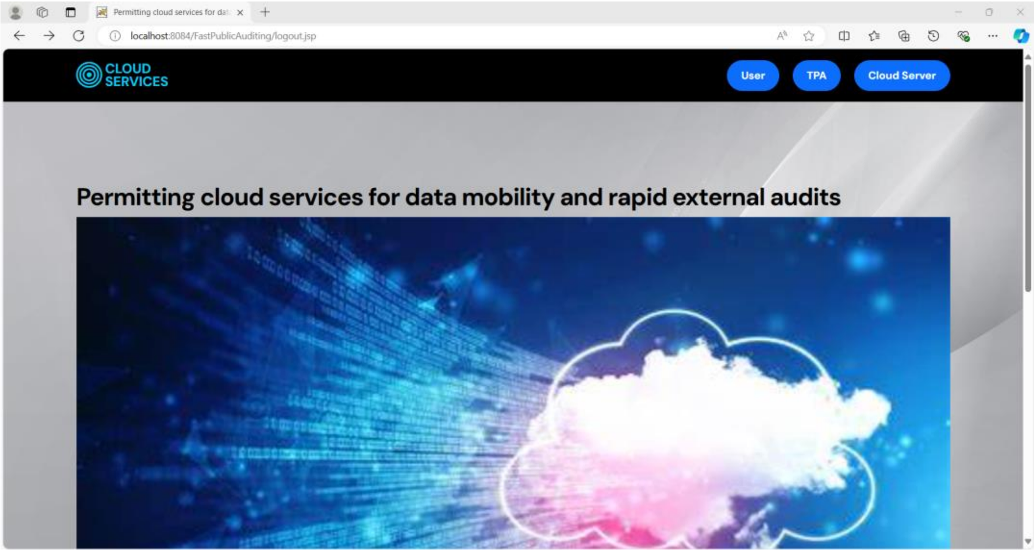

Fig -2: Home Page

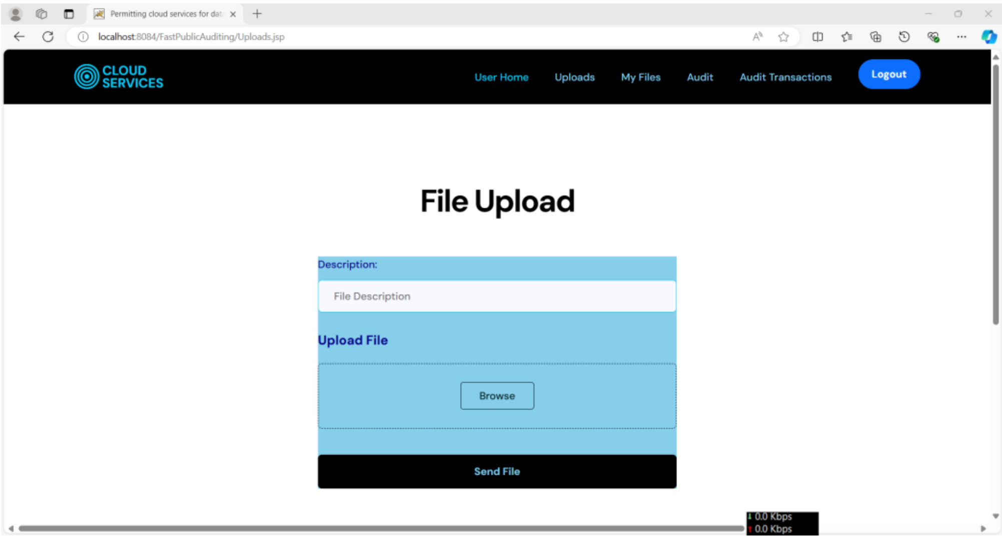

Fig -3 File Upload page

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11756

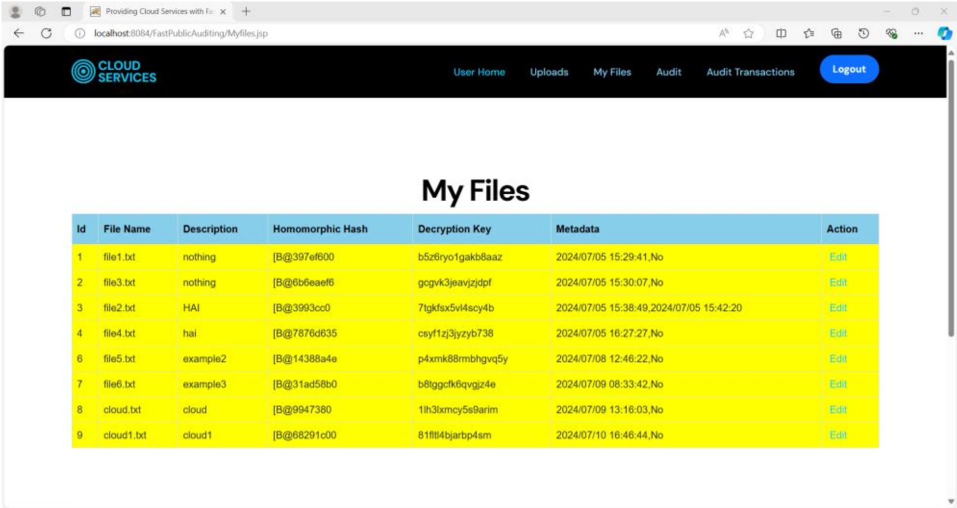

Fig -4: My files page

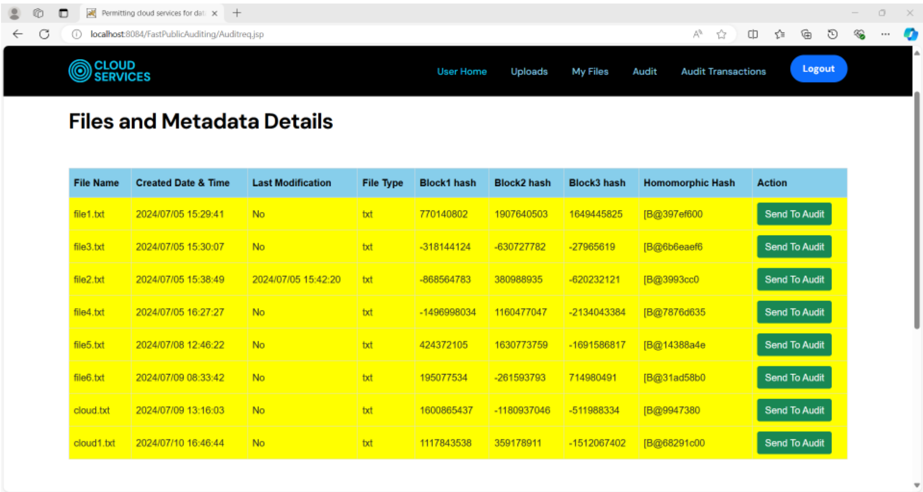

Fig -5: Files Details page

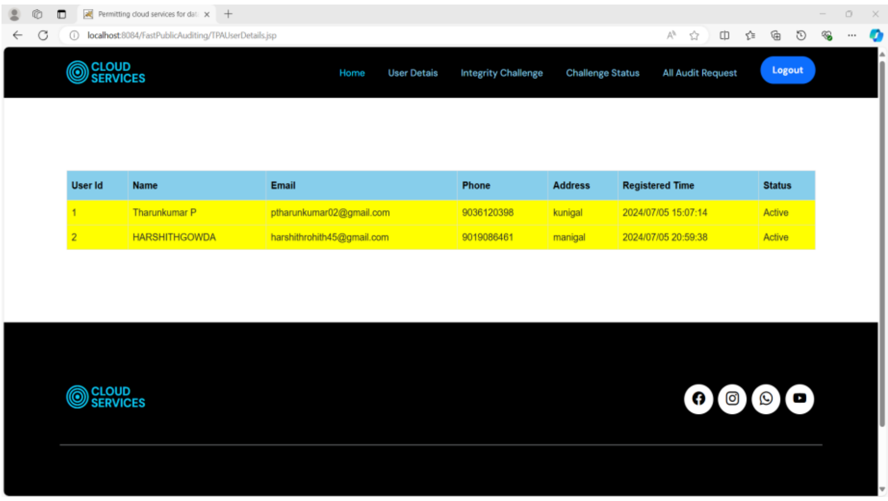

Fig -6: User details Page

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⋡ Peer-reviewed & Refereed journal ⋡ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11756

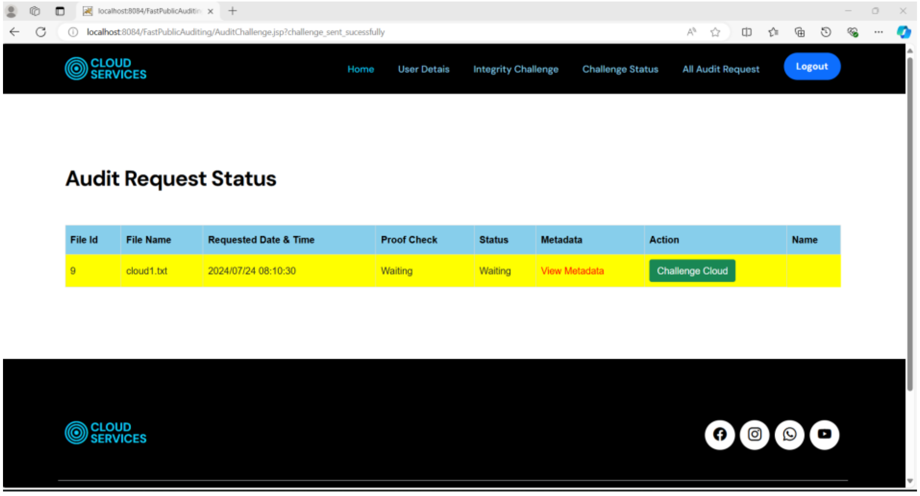

Fig -7: Audit Request Page

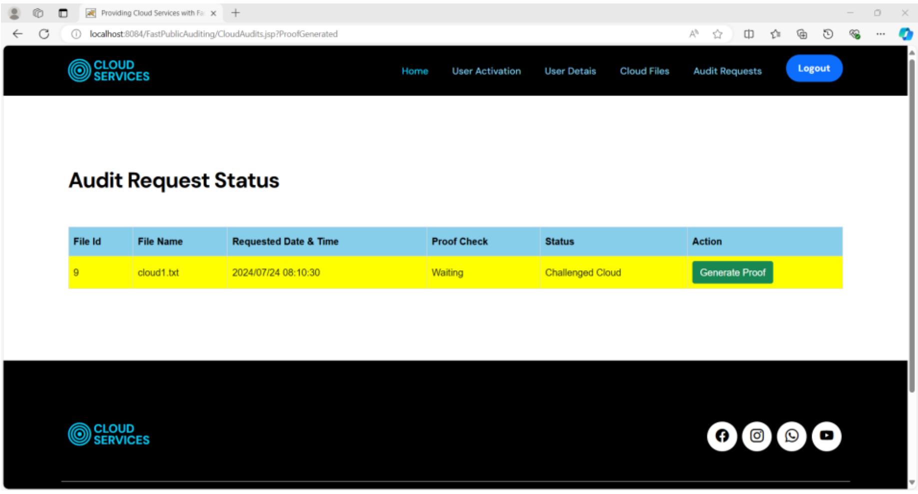

Fig -8: Proof Generating Page

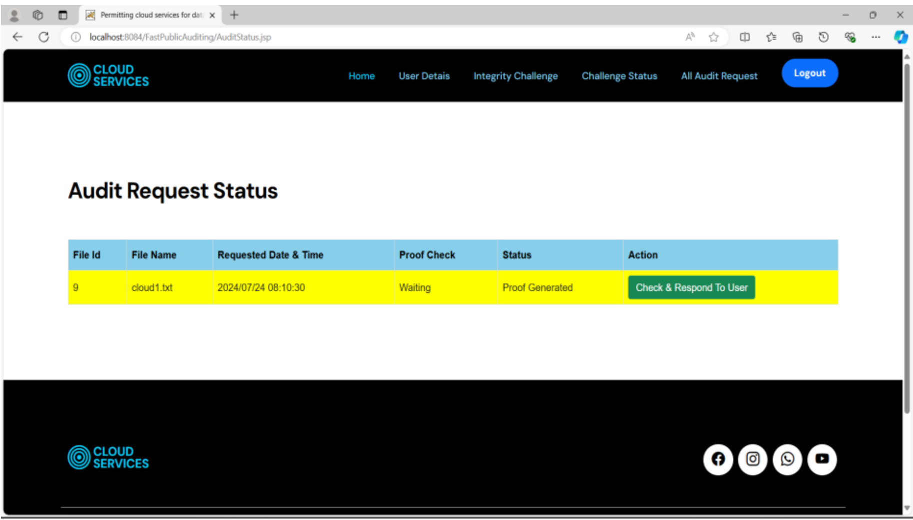

Fig -9: Audit Proof Check page

DOI: 10.17148/IARJSET.2024.11756

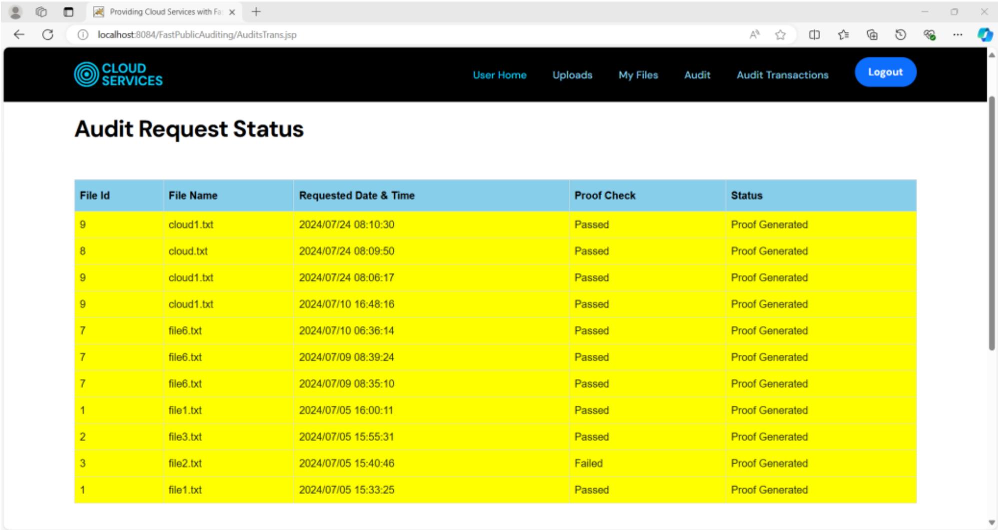

Fig -10: Audit request page

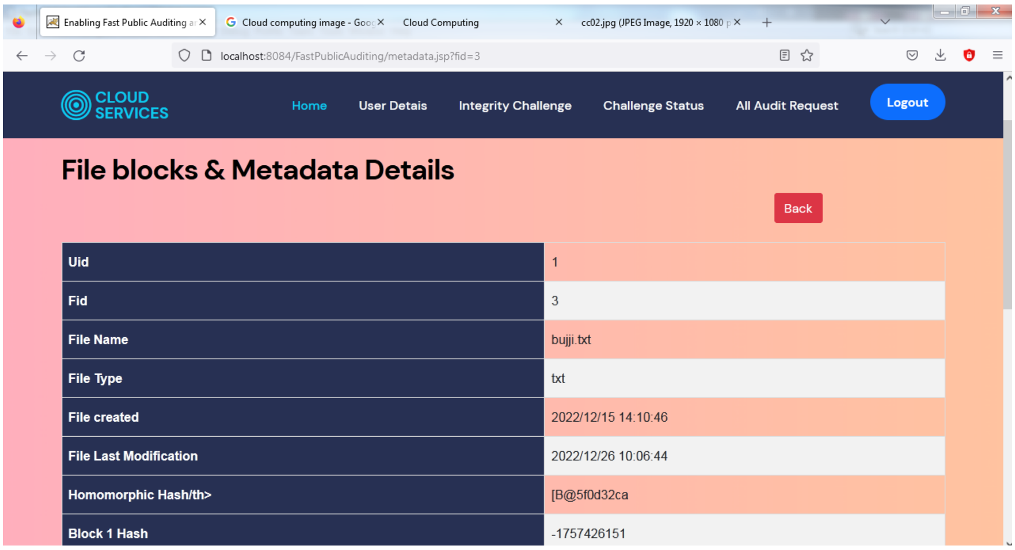

Fig -11: Meta data details page

VI. CONCLUSIONS

We offer an open auditing mechanism for data encrypted that allows exceptionally rapid data dynamics in this work. Regardless of the quantity of blocks, the suggested approach allows data dynamics at a constant cost. Our auditing challenge-response technique necessitates a constant total of pairs and exponentiations, which considerably boosts the auditing results verification speed. The suggested approach protects data confidentiality and integrity while stored on a cloud server. Due to the homomorphic hash function, the TPA may check the accuracy of the evidence during an audit with unlocking it or exposing the key.The suggested system involves minimum extra processing while ensuring privacy of information and integrity, according to reliability and security studies.

REFERENCES

[1] M. Arambrust et al., "A Vision of Cloud Computing," ACM Communications, vol. 53, no. 4, 2010, pp. 50-58.
[2] K. Reen, C. Wanag, and Q. Waang, "Security Concerns for the Public Cloud," IEEE Internet Comput., vol. 16, no. 1, Jan./Feb. 2012, pp. 69-73.
[3] "Cloud safety for the masses," D. Song, E. Shi, I. Fischer, and U. Shankar, Computer, vol. 45, no. 1, pp. 39-45, 2012.

DOI: 10.17148/IARJSET.2024.11756

[4] L. Weii et al., "The safety and privacy for cloud-based data and computation," Inf. Sci., vol. 258, pp. 371-386, 2014.
[5] G. Atenieese et al., "Prrovable data possession at untrusted stores," in Proceedings of the 14th ACM Conf.Comput.Commun.Secur., 2007, pp. 598-609.
[6] R. Di Pietro, G. Ateniese, L. V. Mancini, and G. Tsudik, "Scalabeeleandefficientprovabledatapossession," in Proc. 4th Int. Conf.Secur.PrivacyCommun.Netow., 2008, pp. 1-10.
[7] A. Juels and B. S. KaliskiJr., "PORs: Proofs of retrieevability for large files," in Proc. 14th ACM Conf. Comput. Commun.Secur., pp. 584-597, 2007.
[8] H. Shachaam and B. Waters, "Compaact proofs of retrievability," in Proceedings of the International Conference on Theory, Appl. Cryptology, and Information Security, 2008, pp. 90-107.
[9] C. Erway, A. K€upc u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Trans. Inf. Syst. Secur., vol. 17, no. 4, pp. 1-29, 2015.
[10] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling publicauditability and data dynamics for storage security in cloudcomputing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, May 2010.