A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage.

Doma Bhargav
Final year student,
NWC Department,
SRM Institute of Science & Technology, Kattankulathur
db8482@srmist.edu.in

Upanshu Bhardwaj
Final year student,
NWC Department,
SRM Institute of Science & Technology, Kattankulathur
ub4116@srmist.edu.in

Dr. M. Saravanan,
Associate Professor,
NWC Department,
SRM Institute of Science & Technology, Kattankulathur.
Saravanm7@srmist.edu.in

Abstract— Cloud computing is a fast developing technology that offers extremely quick and inexpensive computer services as well as data storage. Cloud service providers or cloud custodians handle all data saved on cloud servers. on their capacity as data owners, data owners are worried about the legitimacy and dependability of the data kept on the cloud. Any unapproved user or individual has the ability to misuse or modify data. This work suggests a secure public auditing system that makes use of outside auditors to verify the confidentiality, dependability,and integrity of data stored in the cloud. Two public key encryption algorithms are RSA-15360 and SHA-512 integrity checks,and the AES-256 encryption algorithm are all included in this suggested auditing scheme. And carry out data dynamics operations, which primarily deal with addition, removal, and alteration.

Keywords—TPA, CSS, Owner of Data Open the file, Grant Request, Create Key, Download Document…

I.INTRODUCTION

The global cloud computing market is predicted to grow at an annual growth , from $272 billion in 2018 to $624 billion by 2023, according to a research and markets analysis.. In today's world, cloud computing is an advanced technology that everyone uses, whether internally or outside. Cloud computing uses cutting-edge, quickly developing technologies for computation and storage. It makes use of compute and storing in order to serve the lowest possible expenses. Three fundamental services were offered by the service model: (SaaS), (PaaS), and (IaaS).

According to the NIST definition, "Cloud computing is a feasible, on-demand, permissive model that is widely used and provides a shared pool of reconfigurable computing resources (such as networks, servers, storage, apps, and services) that can be released and furnished immediately with minimal hassle from service providers or management." One essential cloud computing service is cloud storage. They include data availability, privacy, protection, and location; one important development in cloud security is secure communication. Cloud computing presents a number of security challenges, including threats, data loss, degradation, outside malicious attacks, and multi-tenancy. The data's integrity is preserved by the cloud system. by preserving the stored information. Unauthorized users shouldn't have access to inaccurate or different data. The cloud computing provider dutifully maintains data reliability and integrity. Because consumers believe that The privacy of data is crucial, they Keep their personal and sensitive information on cloud storage services. In order to guarantee authentication and access management policies, data privacy is taken into consideration. Growing cloud authentication and data confidentiality could propel cloud computing forward. Because of this, data stored on cloud platforms should be protected by security, integrity, privacy, and confidentiality of utmost importance from the standpoint of the user.

The presentation of a data auditing scheme includes a safe cloud computing system for storing data. Owners of the data or TPAs can perform examinations, which are essentially deeper user information checks. Data within the cloud is kept up to date through its integrity. Private audibility, which enables the data owner to assess The accuracy of the data, is one of the two components of TPA management. Nobody is qualified to question the server about how the data is being handled.

II.LITERATURE SURVEY

[1] Vinaya Sarmalkar; Yatin Gandhi; R. Patil Rashmi "Cloud Storage Security Using Deduplication Method 2020" In this paper, we identify several problems, such as the inability to assign a new hash tag to client-side deduplication after file updates. Thus, the tools utilized here are the RDPC protocol, C++, homomorphic hash algorithm, and dynamic ownership, which fails.
In brief: We present an innovative statistically sound plan, guarantee that the problems we observed earlier will be resolved, and prevent the formation of duplicates. We encrypt the data in the file using the AES and SHA algorithms. The data owner's stored data is not accessible to unauthorized parties.

[2]Hemraj Lamkuche, Sunil Kumar, and Dilip Kumar "Cloud Computing Application: Secure-Drive 2021 for Secure File Storage"
We identify a few problems in this paper, which are Safe Data Transfer utilizing secure communication protocols, such as HTTPS, to protect files during upload and download, and making sure that data is kept private while in transit. Here, HTML, CSS, Blowfish, Triple DES, and Phyton are the tools that are used. Cloud-based algorithms were employed.
In brief: the primary benefits of our systems are that they Thus, we offer algorithms that get around these problems and function better. In this case, they merely use a few apps to secure the data, but we use the AES algorithm and TPA to create files that are more secure and prevent other data owners from accessing the data without a key. CSS also

plays a significant part in approving and rejecting the owners' requests.

[3] P. Baby Shamini; K. S. Megavarshini; D. C. Joy Winnie Wise A QR Code-Based Real-Time Auditing System for Safe Cloud Storage in 2020 Concurrency Management: A Look at Mobile Devices These are some of the issues in this paper; while using QR codes to secure the data is an excellent method, there are still a lot of issues that need to be resolved, such as the camera scanner not working properly and the need to take a long time but efficiently to send some keys to a respected mail address. To address these issues, the authors use HTML, CSS, Python, and Apache MariaDB among other tools. MariaDB is the database, and HTML and CSS are used for the website.
In this study, we tackle three important problems related to concurrency control and mobile devices. Thus, the data is not secure because they did not even employ encryption algorithms; instead, it is secured by a single security mechanism known as QR.

[4] T. Longbin; Dai Wenyun. A Framework for Safe and Expandable Key-Value Stores, 2017. It is not possible to transfer queries from one database to another since key-value databases lack a querying language. In this paper, we addressed this issue, which is entirely based on the question. One data base to another receives the data transfer. A key value will be used to access the data, which is primarily focused on scalability. They employed cutting-edge technologies like Google Bigtable, Amazon Dynamo, Python, and flash memory.
Summary: As cloud computing has become more widely used, worries about the security of the data being outsourced have unavoidably increased. Because of the resource limitations of mobile devices, security solutions must send all computing-related tasks to the cloud for execution.

[5] Tanuj Jain, Nidhi Nair, and Mihir Gada Cloud Computing Application for Secure File Storage: Secure-Drive 2021The literature review emphasizes how important safe file storage is when it comes to cloud computing. It examines the fundamental idea of secure transmission as well as the instruments and technologies used to accomplish this. Through an analysis of an application such as "Secure-Drive," which makes use of web development technologies, encryption algorithms, and secure communication protocols, this survey adds to a better understanding of the steps taken to guarantee that data in cloud-based file storage systems is secure and confidential.
Summary: The literature review is lacking in depth, organization, citations, and accurate definitions of technical terms, among other problems. There is a typographical error and an ambiguity regarding the authors' roles. Additionally, a section on future research directions is absent, as are the most recent research updates. To create a better survey, these problems must be fixed.

[6] S P. Calista Bebe, Akila D. Orchini Comparative User Authentication-Based Streebog Hash Function for Safe Cloud 2020 Data Preservation An enhanced comprehension of user authentication and data security in relation to cloud storage is made possible by this survey of the literature. The "Orchini" paper aims to give readers important insights into this developing field by examining the difficulties, datasets, and methodologies used in the study.
Summary: Crucial facets of cloud data security are covered in the paper "Orchini: User Authentication and Streebog Hash Function for Secure Cloud Data Storage" by P. Calista Bebe and Akila D. Nonetheless, it has problems with the intricacy of its title, the need for a more thorough examination of problems and solutions, and the need to define the significance of datasets and acronyms. To improve the overall quality and impact of the paper, additional clarity regarding the methodology and specific contributions is needed.

[7] IK Meenakshi and Sudha George. Employing TPA for Cloud Server Storage Security.2014 issues of International Journal of Advanced Research in Computer Science and Technology (IJARCST), ISSN: 2347-9817.
Data is moved over to a distant cloud server in cloud computing. The owner can always rely on the cloud server to store their data and retrieve it when required. Data integrity in cloud storage is a critical concern since many users store their data there. The owner hopes that after transferring the data to the cloud, their apps and data will be protected. Nevertheless, there's a chance that the owner's data will be lost or changed. For the purpose of validation in this case, the user needs to download the data.

[8] An effective auditing scheme for cloud data storage security was developed by J Agarkhed and R Ashalatha.[ICCPCT, 2017].
Cloud computing is on-demand processing that stores data remotely and services are provided using a communal collection of computer power.The requirement to store and oversee a show is satisfied by cloud computing. A number of remarkable innovations, such as methods that are guide-decline and parallel available for information access and security. The owner also gains from the release of the load of maintaining and storing native data, as well as from no longer having to worry about security and storage. A creative approach is required to guarantee the on-demand data's accuracy is modified and that the cloud owners have had a chance to verify it.A cutting-edge secure cryptography hashing algorithm is used for the encryption and file division. A private and public key are given to the user for reliable data file retrieval after the data is uploaded. A suggested modified RSA cryptosystem algorithm is used to generate those keys. Occasionally, an efficient audit of the data file is conducted using a multilevel hash tree algorithm. The efficacy and effectiveness of the recommended algorithm in comparison to the current algorithm are demonstrated by the implementation and the ensuing outcomes.

III.EXISTING METHOD

Cloud service providers handle all data stored on the cloud. They are concerned about the validity of their data as owners. and dependability of the information stored on a cloud servers. Any unapproved user or person has the ability to misuse or alter data. In the context of cloud computing,

cloud administrators or service providers are in charge of managing data stored in the cloud, abdicating the owners' accountability for its safekeeping. Data owners are worried about the about the legitimacy and dependability of their information kept in the cloud due to this transfer of control. These concerns stem from a number of important factors: data integrity, where any tampering or illegal access could compromise accuracy; ownership, particularly regarding who has ultimate control over the data; and compliance with industry standards and regulations, which frequently mandate strict data storage and privacy compliance.To allay these worries, cloud environments must be equipped with strong security measures, encryption protocols, access controls, and authentication mechanisms. To build trust in cloud-based data storage, data owners must carefully choose and manage cloud service providers, establish guidelines for data usage, and exercise active oversight to guarantee that data is safe and undisturbed.

As an existing method deals with the cloud's custodian or cloud service providers handle all data stored on the cloud. As the owners of the data, Their concerns are with the veracity and authenticity of the information kept on cloud servers. Any unauthorized person or In addition, the user can incorrectly use or alter data.

IV.PROPOSED METHOD

A This auditing proposal integrates the use of the AES-256 encryption algorithm, the SHA-512 integrity checker, and the public key encryption algorithm RSA-15360.. And perform data dynamics tasks., which primarily deal with addition, removal, and alteration.

A thorough strategy for improving data security and integrity is represented by the suggested auditing plan. To accomplish these aims, it integrates three essential cryptographic methods. First, in order to protect the confidentiality of data, AES-256 encryption is used, rendering the data unreadable without the proper decryption key. Second, SHA-512 is used for integrity checks, producing distinct hash values to verify the accuracy of the data and identify any unauthorized modifications. Finally, secure public key encryption algorithm RSA-15360 is used to create secure communication and authentication between parties; this is especially useful when verifying the identity of the sender is essential.

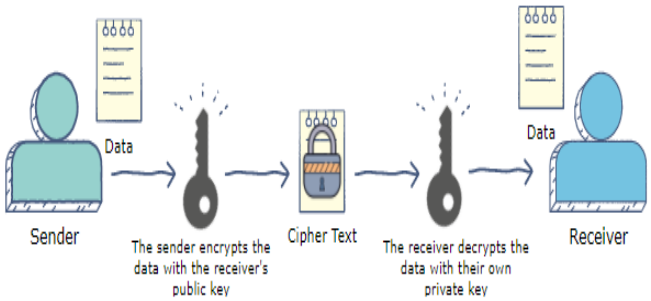
Data dynamics operations like insertion, deletion, and modification are supported by this auditing scheme. These procedures are standard in many applications where data is updated often. Encouraging secure data manipulation, ensuring data integrity, and safeguarding confidentiality are the main goals. It provides a solid method for guaranteeing data security and integrity, even in dynamic data environments.

V.METHODOLOGY

a) Advanced Encryption Standard:

Using this to Encrypt the saved data or file in the cloud storage so the data will be in unreadable format and in the same way it is used to decrypt the data which makes the data readable unique capabilities to identify patterns within images. CNNs are adept at learning local features or patterns within images, such as edges, corners, and textures. Moreover, CNNs possess translation invariance, making it possible for them to identify patterns regardless of their position in the image and their hierarchical structure allows for the learning of complex features by combining simpler ones, making them proficient at understanding image content. With parameter sharing in convolutional layers, CNNs reduce the number of parameters, enhancing efficiency and reducing overfitting risks.

Firstly, the sonar images are passed over to learnable filters which slides over the input sonar images which is responsible for capturing unique and distinct features. Max pooling is used in this case to analyze interspersed between convolutional layers, to decrease spatial dimensions while maintaining the necessary data, enhancing the network's robustness and computational efficiency. Then follows the fully connected layers, where the high-level reasoning takes place based on the flattened feature maps. These layers culminate in an output layer, which produces class probabilities in classification tasks. During training, CNNs learn from labeled data by minimizing a loss function, optimizing filter weights and biases through gradient descent and backpropagation. This iterative process continues until the model achieves satisfactory performance.



b) Rivest-Shamir-Adleman:

In order to safeguard encryption keys and secure communication channels, RSA is a popular asymmetric encryption algorithm used for digital signatures and key exchange.Forests.

The RSA (Rivest-Shamir-Adleman) asymmetric encryption algorithm is essential to a cloud storage project. It fulfills a number of purposes that are crucial to the integrity and security of data. It first establishes secure communication channels by facilitating secure key exchange. Furthermore, it facilitates the creation of digital signatures, thereby

authenticating and maintaining the integrity of data. Last but not least, RSA improves privacy and data security in dynamic data operations. In conclusion, RSA is essential for guaranteeing data authenticity and secrecy in cloud storage projects that involve safe data dynamics and open auditing.

c) Secure Hash Algorithm 256-bit

Data checksums or hashes are computed using the cryptographic hashing algorithm SHA-256 to ensure data integrity.

SHA-256, or Secure Hash Algorithm 256-bit, is an essential part of an auditing plan for cloud storage that is both public and dynamically secure project. Since it creates distinct digital fingerprints, or hashes, for data, SHA-256 is essential for guaranteeing data authenticity and integrity. Particularly in dynamic cloud storage environments where data is constantly changing, these hashes are used to confirm data integrity. SHA-256 is a vital tool for preserving the dependability and credibility of data throughout its lifecycle in the cloud because of its capacity to offer real-time verification of data integrity and its participation in public auditing schemes.

VI.IMPLEMENTATION

a) Data Owner:

The data owner is essential in guaranteeing the security and integrity of their data saved in the cloud under a secure data dynamic and public auditing scheme. There are numerous obligations such as Data Import It is the data owner's responsibility to safely upload their data to the cloud storage service. To safeguard the data while it is in storage, this may entail access control and encryption techniques. Establish policies and access controls to limit who can view and alter data stored in the cloud. Defining user roles and permissions, audit preparation to create and maintain metadata, and audit information for the data may all be part of this. Over time, the integrity of the data can be confirmed using this metadata. Procedures to verify the accuracy of the data that has been stored are started by routine auditing. As a response to audit challenges, this may entail comparing the metadata created or the stored data with the original data. If a third party or cloud service contests the data's integrity, the data owner must present proof of data integrity derived from the metadata that has been stored. Important Prior to now, management Oversee and rotate the encryption keys that are used to protect the data, keeping an eye on them and sending alerts when necessary. Keep an eye out for any unusual activity or illegal access to the cloud storage service.

And it has different module.

Register: The owner of the data may register and log in using proper credentials.

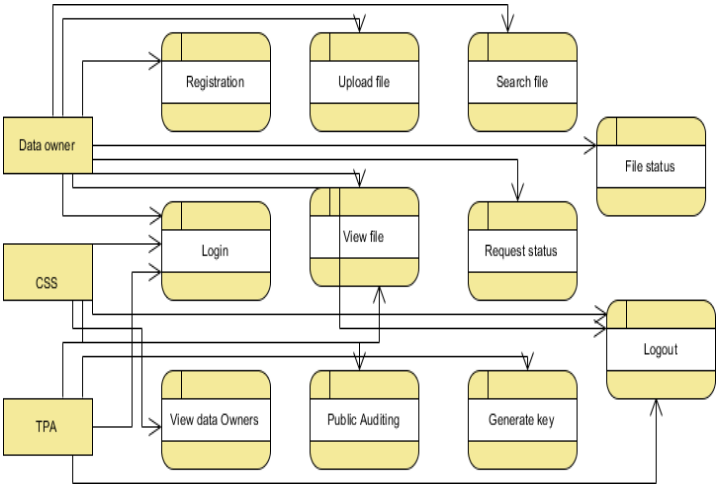
File Upload: The data supplier is able to upload the file.

View File: The data owner can check if a file was uploaded correctly by viewing it once.

File Search: A user can perform a keyword-based search to find a file. If the file is found, the user can view it and send a request to the cloud to download it.

View File Status: The individual submitting the request has the ability to see the file's status.

Request Status: After the cloud and TPA have accepted the request.



b) Cloud provider login:

It requires multiple steps. I will explain in detail below:

Lists of controls over access (ACLs) Control who can read, write, and alter data by implementing access control lists. As access rights are modified, these lists should be periodically checked and updated.

Versioning of your data can help you monitor changes over time. Make sure this feature is enabled. When updating dynamic data, this is crucial.The application of cryptographic hashes or checksums can guarantee data integrity.. To find any illegal modifications, periodically compare data to these integrity checks.

Digital Signatures: To ensure the authenticity of data, use digital signatures. To ensure that the information hasn't been altered during transmission, this is essential.

Continual Evaluations: Audit your cloud storage on a regular basis to look for any irregularities or unapproved access. External auditors as well as your company are capable of doing this.

Secure Communication: Make sure that your systems and the cloud provider are communicating in a secure manner at all times. To secure data while it's in transit, use VPNs and HTTPS protocols. Install security updates on a regular basis to minimize potential vulnerabilities in your systems and cloud services.

c) Third party authority:

When it comes to confirming the accuracy and consistency of data kept in the cloud, a third-party authority usually plays a pivotal role in a dynamic, safe, and open auditing system. which usually is a separate organization that the user and the cloud provider trust, becomes involved. Public keys or user and cloud provider credentials may be in the possession of this authority. Additionally, it has various modules:

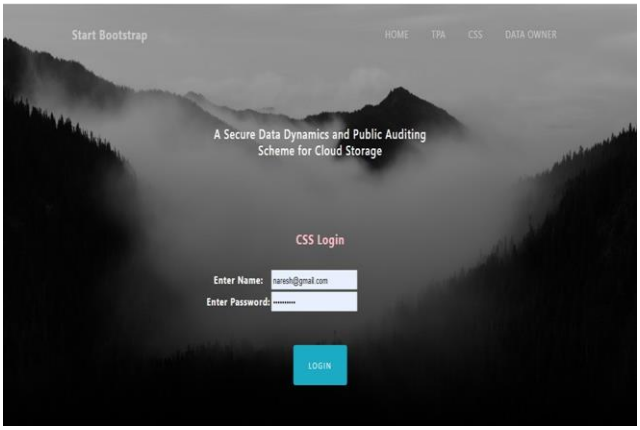
Authorize owners by logging in.

Generate key to user: An owner's specific key is generated by authority.

VII. Results

Home page: Protected data dynamics and open auditing system for cloud storage homepages

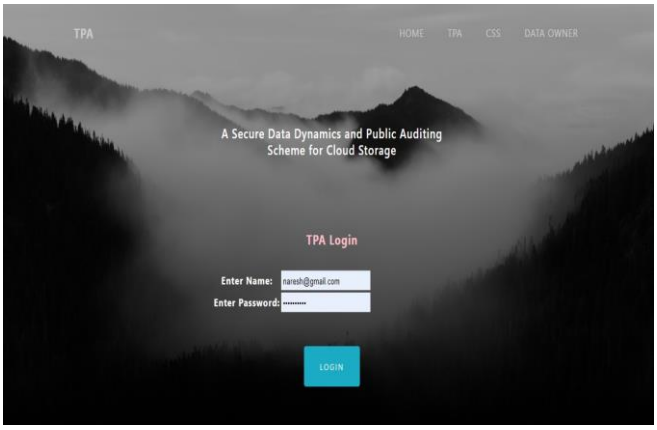
CSS Login: Cloud provider can login with his/her credentials



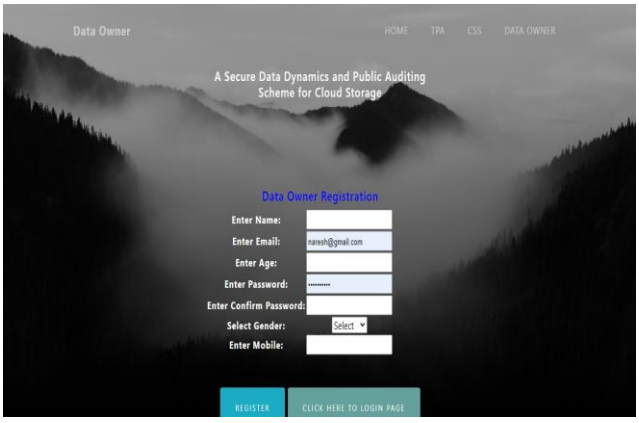
CSS Home page: After login home page for CSS

View all data owners: Cloud can view all the data owner details to givepermission.

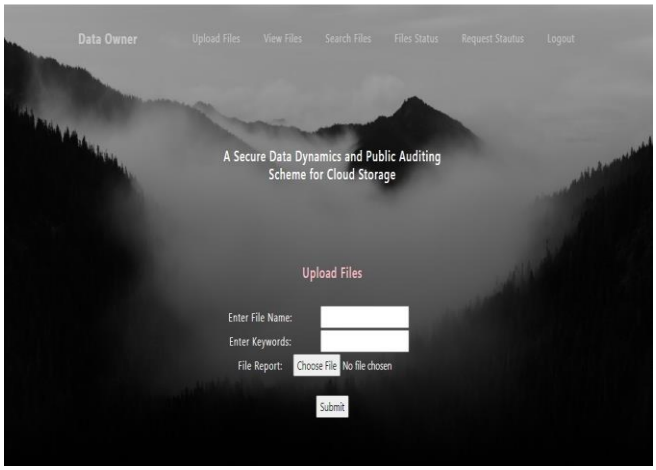
TPA Login page: Authorize owners by logging in with a third-party authority.



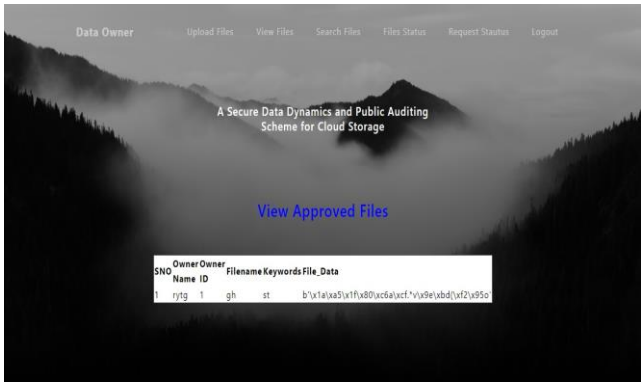
Data owner registration page: Data owners can register and log in using legitimate credentials.



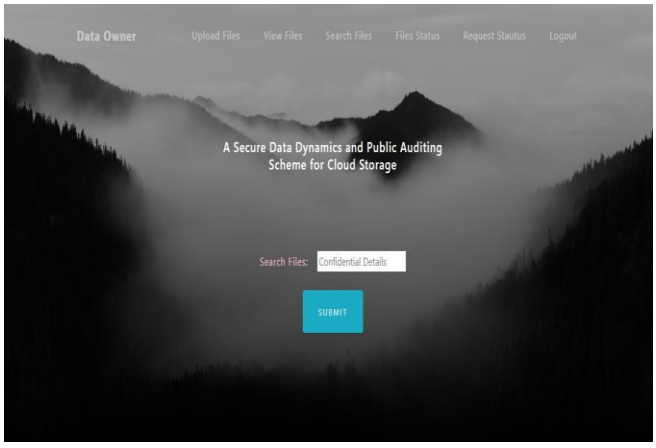
Upload data: Data provider can upload the file.



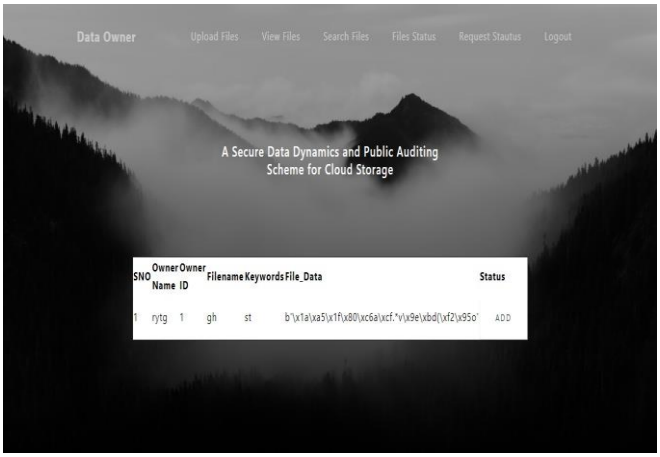
View files: Data Owner can check uploaded file whether the file is correctly uploaded or not.



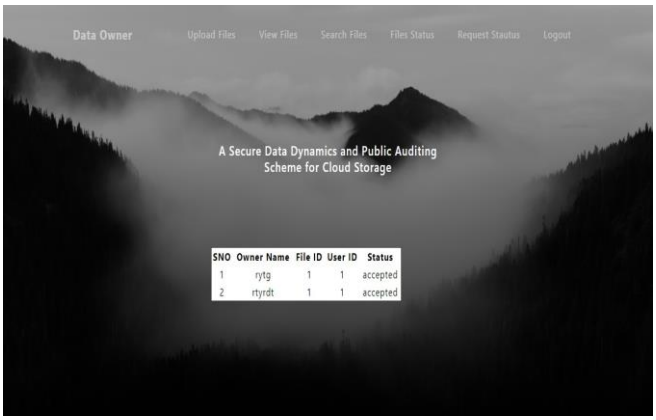
Search files: A data user can use a keyword to search for a file; if the file is found, the user can view it and request that it be downloaded from the cloud.



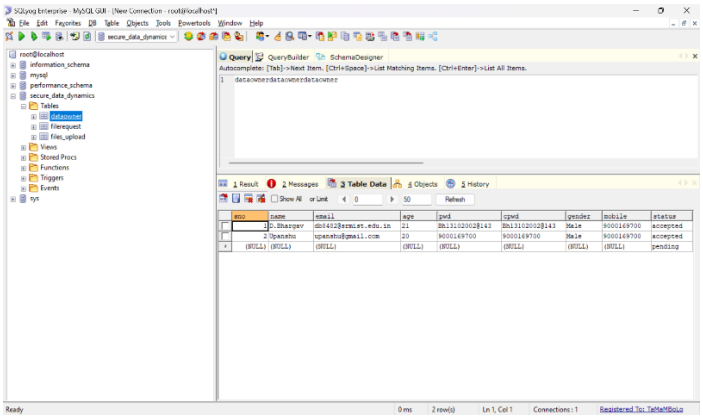
View data: After search the data we can view.



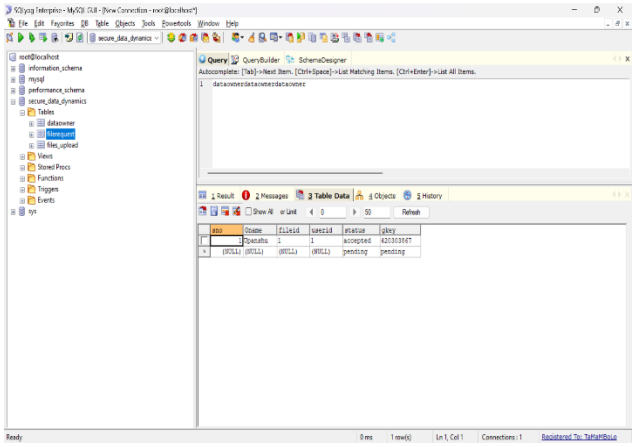
File status: The person who is sending request he /she can view the status of that file.



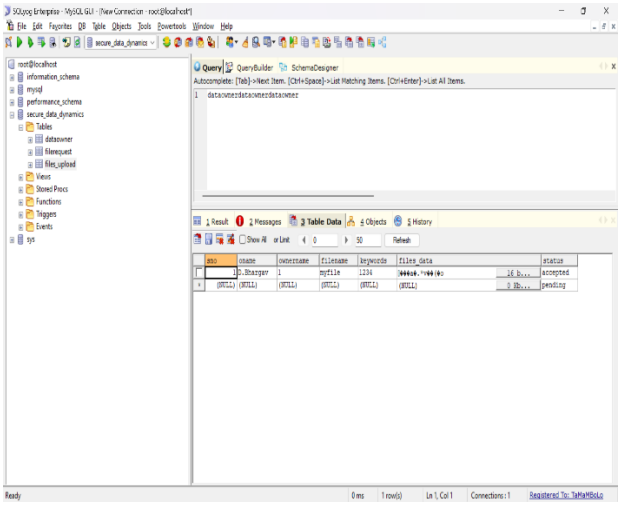
Data Owner Registraion table:



Request table:



Files Upload:



VIII.CONCLUSION

In conclusion, our study on Safe data dynamics and open auditing system for cloud storage gave the idea on, Storing the data securely on the cloud is one way to conduct a secure audit. The AES-256, RSA-15360, and SHA-512 The potential uses algorithms to guarantee that TPA cannot access data related to the robustness auditing scheme. We suggest an procedure for data dynamics that focuses on deals with insertion removal, as well as altering. Then, the CSS should grant the data owner's request. The key that the owner needs to access the data is generated by the TPA. There is potential use for this application in the software industry.

IX.FUTURE ENHANCEMENT

In future we would like to carry out data auditing in batches. One efficient way to guarantee data security and integrity in cloud storage environments is to implement the Safe Data Dynamics and Open Auditing Program for Cloud Storage. To further increase its usefulness, improvements can be made in a number of areas in the future. These improvements might involve the use of distributed storage systems for improved fault tolerance and scalability, the integration of sophisticated encryption algorithms to fortify data protection, the deployment of more resilient access control mechanisms to thwart unauthorized access, and the application of machine learning techniques for anomaly detection and intrusion prevention. Blockchain technology integration could also help the plan by offering a decentralized, impenetrable audit trail that would increase accountability and transparency.

X.REFERENCES

[1] The global cloud computing market report 2019.

[2] J Agarkhed, R Ashalatha-"An efficient auditing scheme for data storage security in cloud".2017[ICCPCT].

[3]. SK Saroj, G Noida, SKChauhan, AK Sharma "Threshold cryptography based data security in cloud computing".S Vats-2015.

[4] Mell, Peter, and Tim Grance.The NIST definition of cloud computing(2011).

[5]]P.Mell and T.Grance,"The NIST definition of cloud computing",National Institute of Standards and Technology,Tech. Rep.,2009.

[6].SwapnaliMorea, SangitaChaudhari,"Third Party Public Auditing Scheme for Cloud Storage ",International Journal of Prpcedia Computer Science ,Volume 79,pp.69-76,2016.

[7] Zissis, Dimitrios, and DimitriosLekkas. Addressing cloud computing security issues. Future Generation computer systems 28.3(2012):583-592.

[8] B.L Adokshaja, and S.J.Saritha,"Third Party Public Auditing on Cloud Storage using the Cryptographic Algorithm"ICECDS-2017.

[9]Cong Wang, Sherman SM Chow, Qian Wang, KuiRen, and WenjingLou."Privacy Preserving Public Auditing for Secure Cloud Storage.http://eprint.iacr.org/2009/579.pdf.

[10] Cong Wong, Sherman S M Chow, Qian Wang, KuiRen, and Wen jing Lou."Privacy Preserving Public Auditing for Secure Cloud Storage". IEEE Transactions on Computers, Volume 62, ISSUE 2, February 2013.

[11]AbhishekMohta, Ravi Kant Sahu, Lalit Kumar. "Robust Data Security for Cloud while using Third Party Auditor". International journal of advanced research in CSE (IJARCSE), Volume 2, Issue 2, February 2012.

[12] IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA.International Journal of Advanced Research in Computer Science and Technology (IJARCST) ISSN: 2347-9817, 2014.

[13] Qian Wang, Cong Wang, KuiRen, and Wenjing Lou, and Jin Li. Enabling Public Auditability and Data Dynamics for Security in Cloud Computing. Parallel and Distributed Systems, IEEE Transactions on,22(5):847-859,2011.

[14] KanYang,XiaohuaJia.”An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE Transaction on (1- 10), 2012.

[15] W.Stalling,”Cryptography and network security,”LPE Sixth Edition,ISBN-978-013-335-4690. [16] Kerry Maletsky,”RSA vs ECC comparison for embedded system”Atmel8951.

[17] MeilianaSumagita,ImamRiadi,”Analysis of secure hash algorithm(SHA) 512 for encryption process on web based application”IJCSDF-7(4):373- 381.

ssm

ORIGINALITY REPORT

12%	7%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Heqing Song, Jifei Li, Haoteng Li. "A Cloud Secure Storage Mechanism based on data dispersion and encryption", IEEE Access, 2021 Publication	1%
2	R.Vijaya Manikandan, K. Gurunathan, D. Ravindran, M. Sanjai, V.P. Pranav Raja. "An Novel Algorithm for Cloud Secure Storage Using Cloud Dispersion and Block Chain System", 2023 4th International Conference on Signal Processing and Communication (ICSPC), 2023 Publication	1%
3	Submitted to Harrisburg University of Science and Technology Student Paper	1%
4	Submitted to Southern Methodist University Student Paper	1%
5	"6G Enabled Fog Computing in IoT", Springer Science and Business Media LLC, 2023 Publication	<1%

	Student Paper	1%
10	www.ijcspub.org Internet Source	1%
11	Submitted to Gitam University Student Paper	<1%
12	Submitted to Higher Education Commission Pakistan Student Paper	<1%
13	Submitted to JNTUA College of Engineering, Anantapur Student Paper	<1%
14	www.coursehero.com Internet Source	<1%
15	Submitted to Asia Pacific International College Student Paper	<1%
16	Submitted to Harare Institute of Technology Student Paper	<1%
17	Submitted to Stanmore College Student Paper	<1%
18	ftp.tutorialspoint.com Internet Source	<1%
19	ijates.com Internet Source	<1%