e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

CLOUDGUARD: ENHANCING SECURITY AND PRIVACY THROUGH PUBLIC AUDITING IN CLOUD STORAGE

Gauri Sunilrao Gulwade[*1], **Pooja Vinod Tayde**[*2], **Sneha Raju Jiddewar**[*3], **Shaikh Adnan Zaki**[*4]

[*1,2,3,4]Final Year Student, Department Of C.S.E, Jawaharlal Darda Institute Of Engineering And Technology, Yavatmal, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS51932

ABSTRACT

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly

Keywords: Data Storage, Privacy-Preserving, Public Auditability, Cryptographic Protocols, Cloud Computing, Cloud Service Privacy.

I. INTRODUCTION

Cloud computing is seen as the next big thing in information technology for businesses. It offers many advantages like being able to access services whenever needed, accessing them from anywhere, and pooling resources. It also allows for quickly scaling up or down resources, paying only for what you use, and shifting some risks to the cloud provider. This technology is changing how businesses use IT. One important change is that data is now often stored centrally or outsourced to the cloud. For users, whether they're individuals or companies, storing data in the cloud has its perks. It takes away the hassle of managing storage, allows access to data from anywhere, and saves money by not having to invest in hardware, software, or maintenance personnel.

Cloud computing offers great benefits, but it also brings new security challenges for users' data. When users store data in the cloud, they're essentially handing over control to the cloud service provider (CSP). This means the safety of their data is at risk. Even though cloud infrastructures are robust, they're still vulnerable to various threats like cyber attacks and system failures.

Furthermore, CSPs might have reasons to mishandle users' data, like freeing up storage space or maintaining their reputation. So, while storing data in the cloud is cost-effective, it doesn't guarantee data integrity and availability. Traditional methods of securing data, like using encryption, aren't straightforward in the cloud. Simply checking data integrity by downloading it isn't practical because it's expensive and doesn't guarantee all data's correctness. Plus, it might be too late to fix any issues once data corruption is detected.

Using cloud services is great because it's convenient and saves money. But, it also comes with risks. When you store your data in the cloud, you give up control over it. That means someone else (the cloud service provider) is in charge of keeping your data safe.

Sometimes, bad things can happen to your data even though cloud systems are usually pretty good. There could be computer problems or someone might try to steal your data.Also, the company that runs the cloud service might do things that aren't good for your data, like deleting it to save space or not telling you if something goes wrong. So, even though it's cheaper to use the cloud, your data might not always be safe.

And it's not easy to check if your data is safe in the cloud. Traditional ways of keeping data safe, like using passwords, don't work the same way in the cloud. Just checking your data by downloading it can be expensive and might not even catch all the problems.

II. METHODOLOGY

2.1 THE SYSTEM AND THREAT MODEL

Entities Involved:

Cloud User:

- Holds large amounts of data files to be stored in the cloud.
- Cloud Server (CS): Managed by the cloud service provider, provides data storage service, and possesses significant storage space and computation resources.

Third-Party Auditor (TPA):

- Trusted by the user to assess the cloud storage service reliability on behalf of the user. TPA has expertise and capabilities that users do not have.

User's Dependence on CS:

- Users rely on CS for cloud data storage and maintenance.
- Users may interact with CS to access and update their stored data for various application purposes.

Importance of Data Integrity:

- As users do not possess their data locally, ensuring correct storage and maintenance by CS is critical.
- Data integrity threats can arise from internal and external attacks at CS, including software bugs, hardware failures, network issues, economically motivated hackers, and management errors.

Role of TPA:

- Users may employ TPA to ensure the storage integrity of their outsourced data, reducing computation and online burden.
- TPA conducts periodic storage correctness verification on behalf of users.

Concerns Regarding Data Privacy:

- Users aim to keep their data private from TPA while ensuring its integrity.
- Neither CS nor TPA has incentives to reveal user data to external parties.
- Regulations like HIPAA mandate CS to maintain users' data privacy.
- Financial incentives exist for CS to protect user data as it constitutes their business asset.

Assumptions about Entity Behavior:

- Neither CS nor TPA has motivations to collude during the auditing process.
- The protocol execution is followed without deviation by any entity.

Authorization for Audit:

- Users issue a certificate on TPA's public key to authorize CS to respond to audits delegated to TPA.
- All audits from TPA are authenticated against this certificate.

2.2 Goals for Privacy-Preserving Public Auditing in Cloud Data Storage:

- **Public Auditability:**

Enable TPA to verify cloud data correctness on demand without accessing the entire data or adding extra burden to users.

- **Storage Correctness:**

Ensure no dishonest cloud server can deceive TPA's audit without genuinely storing users' data intact.

- **Privacy Preservation:**

Guarantee that TPA cannot infer users' data content from audit information collected.

- **Batch Auditing:**

Provide TPA with secure and efficient auditing capabilities to handle multiple auditing requests from numerous users simultaneously.

- **Lightweight:**

Allow TPA to conduct audits with minimal communication and computation overhead.

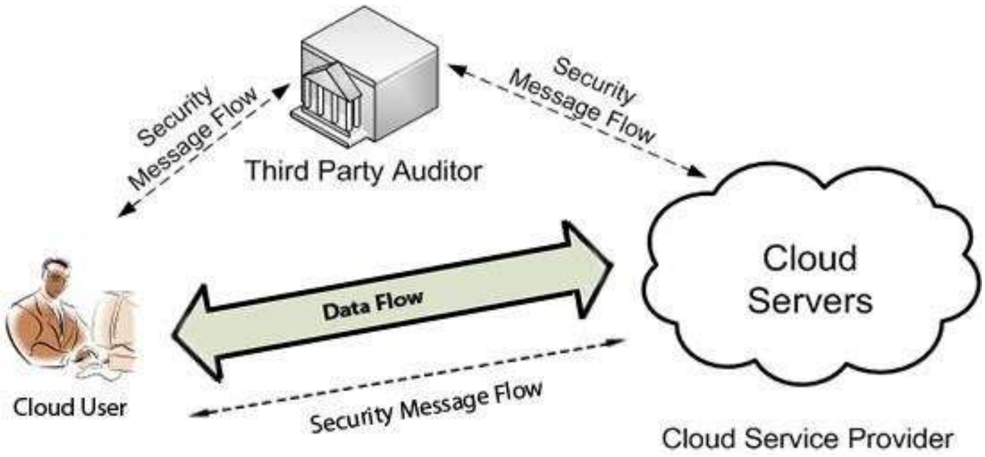


Fig 1: The architecture of cloud data storage service

III. PROPOSED SCHEMES

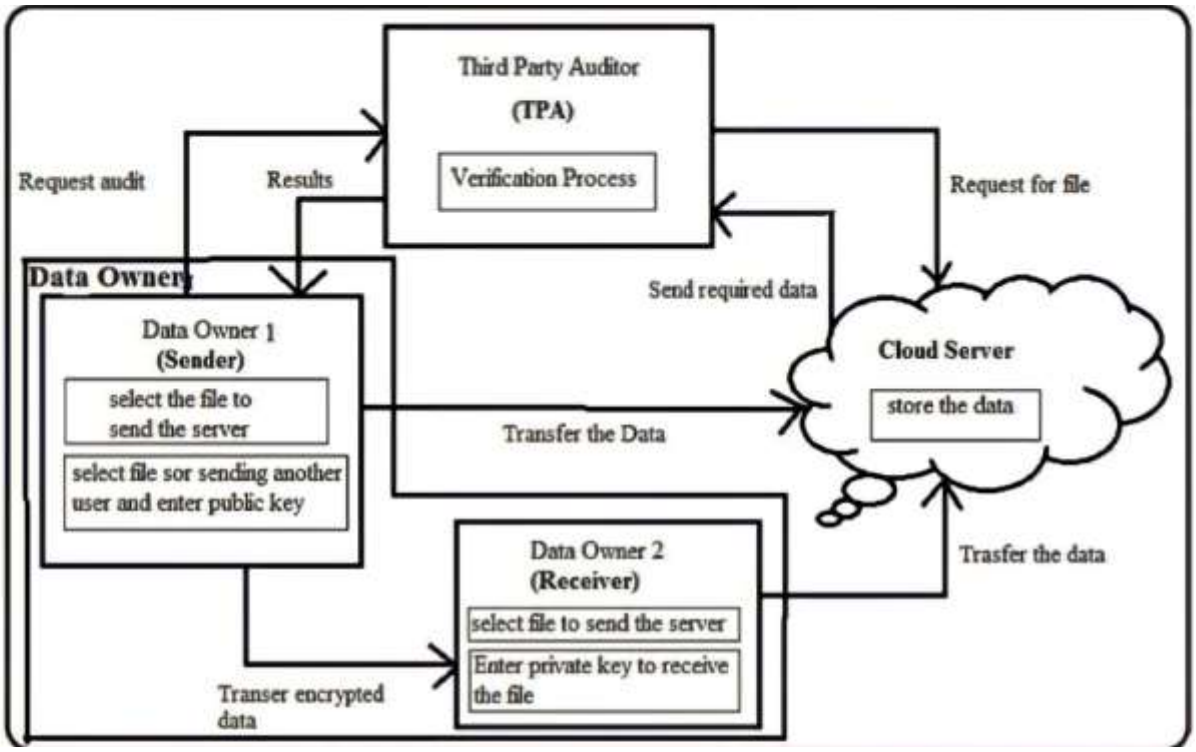


Fig 2: Proposed Auditing Scheme Architecture.

The proposed auditing scheme aims to provide a comprehensive solution for verifying the integrity of outsourced data while addressing various practical considerations such as efficiency, scalability, privacy, and adaptability to changing data.

The proposed scheme consists of three basic entities; they are

1. Data owner: Data owner is an important part of our proposed system. It performs most of the responsibility related to the data. In the proposed auditing scheme, the data owner first performs login and registration with cloud server and TPA. The new user has to firstly register itself by filling the registration form and be the active member of the system. A message for successful registration will be provided. If a user is already

the member of the system then he or she can perform login process. If the user name and password exist in the database, then they will be login successfully for being valid users or else they will receive an error message.

2. Cloud server storage: Cloud server stores the data which is transferred by data owner and send the requested data to the third party auditor.
3. TPA: In the proposed scheme, to perform the task of data auditing a TPA is been used for this purpose. TPA performs data auditing either periodically or on demand by the client. On receiving the auditing request from user or data owner, the TPA starts its auditing process. Later it compares the two signature in verification process. If it matches then it means the integrity of data is maintained and otherwise not maintained. This means that data is not been tampered or changed. The results for the same is provided to the data owner by the TPA.

3.1 THE BASIC SCHEMES

MAC-based Solution

This scheme uses Message Authentication Codes (MACs) to authenticate data. In the first approach, data blocks along with their MACs are uploaded to the server, and the corresponding secret key is sent to the Third-Party Auditor (TPA). However, this approach has drawbacks such as high communication and computation complexities and requires the TPA to know the data blocks for verification. To avoid this, another approach restricts verification to equality checking by precomputing MACs for the entire data file and sending them to the TPA. The TPA then asks for fresh MACs for comparison during audits. While this approach is privacy-preserving, it has severe drawbacks: limited auditing times, state maintenance between audits, and inability to support dynamic data efficiently.

HLA-based System

This system is based on Homomorphic Linear Authenticators (HLAs), commonly used in proof of storage systems. However, existing HLA-based systems are not privacy-preserving.

The analysis of these basic schemes highlights the limitations and challenges. The main scheme, based on a specific HLA scheme, overcomes these drawbacks.

3.2 Privacy-Preserving Public Auditing Scheme

Overview:

The scheme integrates a homomorphic linear authenticator with a random masking technique.

During the audit process, the server's response includes a randomly masked linear combination of sampled data blocks, making it impossible for the Third-Party Auditor (TPA) to derive the actual data content.

Scheme Details:

Setup Phase: The cloud user generates public and secret parameters, including a signing key pair and random elements. These parameters are used to compute authenticators for the data blocks.

Audit Phase: The TPA verifies the signature on the file identifier and retrieves the file's name. Then, it challenges the server by specifying randomly chosen blocks to be audited. The server responds with a proof of data storage correctness, including a randomly masked linear combination of the sampled blocks and an aggregated authenticator.

Verification: The TPA validates the server's response by checking a verification equation. This equation ensures that the response is consistent with the randomly chosen blocks and their authenticators.

Properties:

- The scheme achieves public auditability without requiring secret keying material or states to be maintained by the TPA.
- Privacy is ensured by using random masking to hide the linear combination of data blocks.
- The scheme provides a constant communication overhead for the server's response during the audit, regardless of the number of sampled blocks.

IV. RESULTS AND DISCUSSION

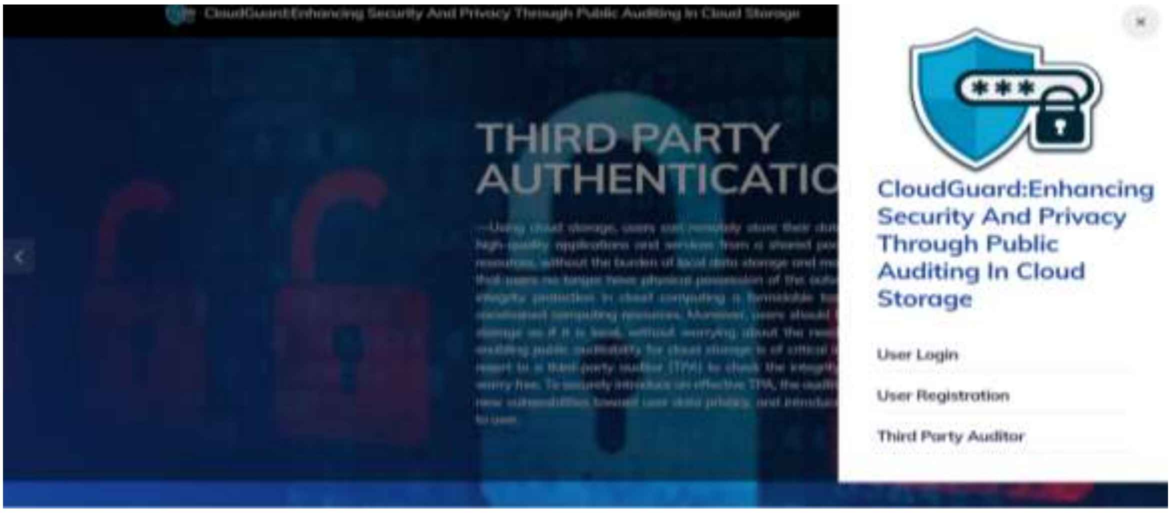

CloudGuard:Enhancing Security And Privacy Through Public Auditing In Cloud Storage
THIRD PARTY AUTHENTICATIO
CloudGuard:Enhancing Security And Privacy Through Public Auditing In Cloud Storage
User Login
User Registration
Third Party Auditor

Fig 3: Home Page

Figure, shows home page of privacy preserving public auditing for secure cloud storage system. It is the first page of working system. When user clicks on upper right side three horizontal line icon on the home page, the main links of working system are open and the links are; user login, user registration and third party auditor.

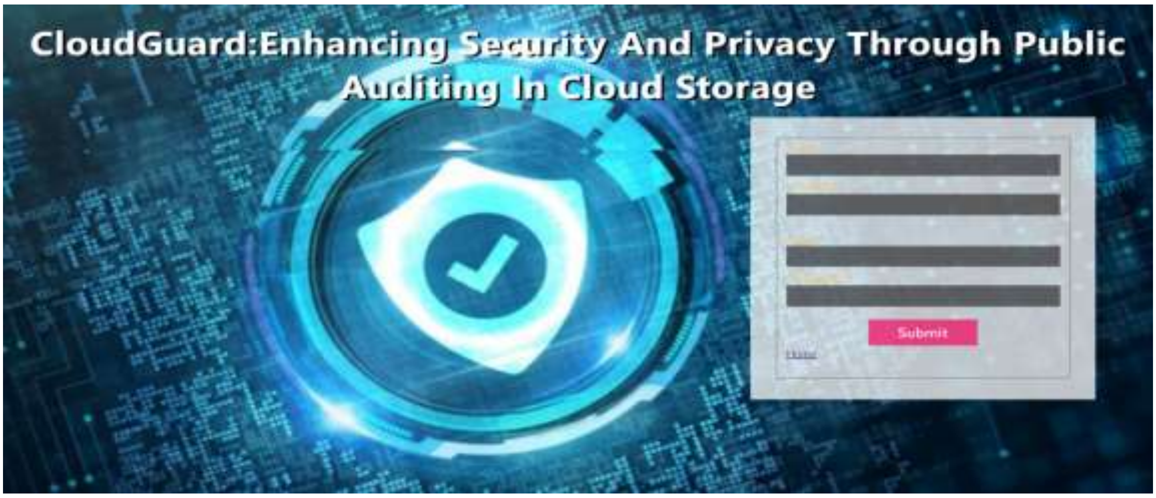
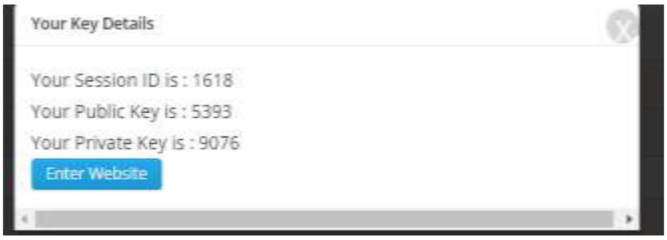

CloudGuard:Enhancing Security And Privacy Through Public Auditing In Cloud Storage
Submit
Home

Fig 4: User Registration

Figure shows User Registration form. When there is a new user to the system, first of all user have register their self. When user clicks on user registration on main link, this registration form will be open. When user enters the system , then they have to authenticate their self. Once registration of user is completed users are allow to authenticate their self.



Your Key Details

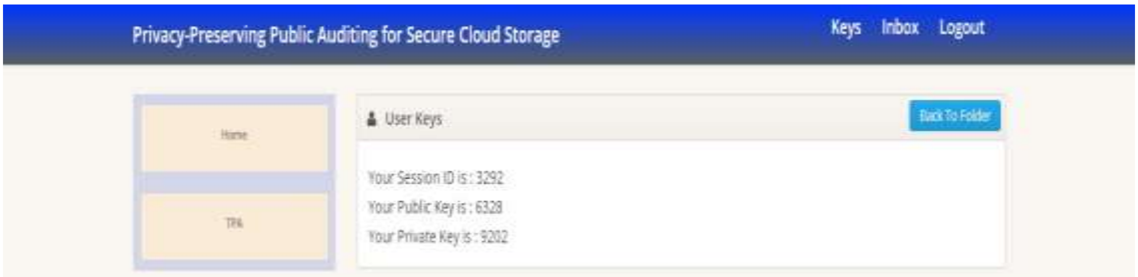
Your Session ID is : 1618

Your Public Key is : 5393

Your Private Key is : 9076

Fig 5: Public key and Private key generation

Shows public and private key generation. When one user want to send any message or any file to another user. This system provide security to the communication by using RSA algorithm. When one user wants to communicate with another user, at that time dynamic public and private keys are generated.



Your Session ID is : 3292
Your Public Key is : 6328
Your Private Key is : 9202

Fig 6: Dynamic key Generation

- There is a one tab in project folder called keys user can able to see there dynamically generated keys in the tab

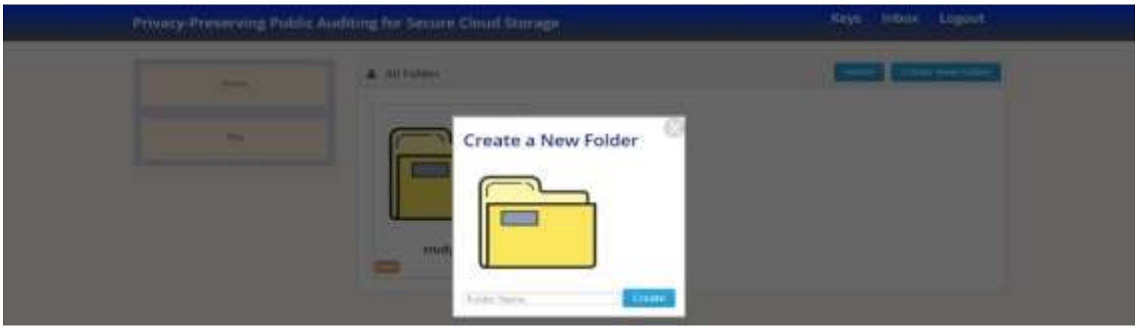
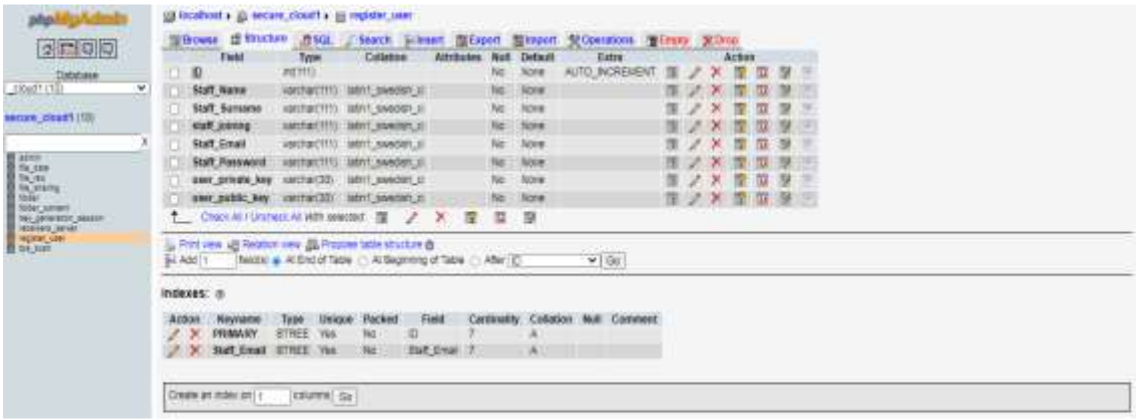


Fig 7: Create Folder

Shows Create folder page. When user wants to create a new folder, then by click on create new folder, a new folder is created.



localhost › secure_cloud1 › register_user

Field	Type	Collation	Attributes	Null	Default	Extra
ID	int(111)			No	None	AUTO_INCREMENT
Staff_Name	varchar(111)	latin1_swedish_ci		No	None	
Staff_Surname	varchar(111)	latin1_swedish_ci		No	None	
staff_joining	varchar(111)	latin1_swedish_ci		No	None	
Staff_Email	varchar(111)	latin1_swedish_ci		No	None	
Staff_Password	varchar(111)	latin1_swedish_ci		No	None	
user_private_key	varchar(30)	latin1_swedish_ci		No	None	
user_public_key	varchar(30)	latin1_swedish_ci		No	None	

Check All / Uncheck All With selected:

Print view Relation view Propose table structure

Add 1 field(s) ● At End of Table ○ At Beginning of Table ○ After ID Go

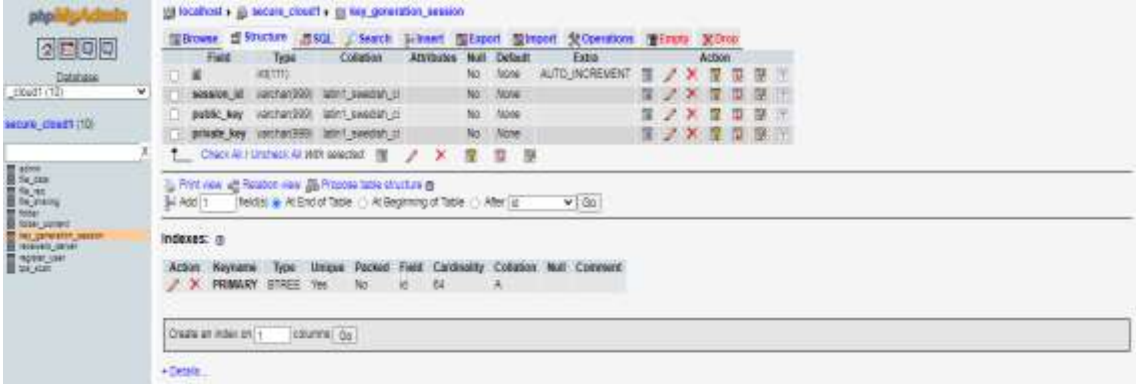
Indexes:

Keyname	Type	Unique	Packed	Field	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	ID	7	A		
Staff_Email	BTREE	Yes	No	Staff_Email	7	A		

Create an index on 1 columns Go

Fig 8: registered USER table structure

Figure shows structure of Register user table. It has eight columns and they are; id, staff name, staff surname, staff joining, staff email, staff password, user private key, user public key.



localhost › secure_cloud1 › key_generation_session

Field	Type	Collation	Attributes	Null	Default	Extra
id	int(111)			No	None	AUTO_INCREMENT
session_id	varchar(300)	latin1_swedish_ci		No	None	
public_key	varchar(300)	latin1_swedish_ci		No	None	
private_key	varchar(300)	latin1_swedish_ci		No	None	

Check All / Uncheck All With selected:

Print view Relation view Propose table structure

Add 1 field(s) ● At End of Table ○ At Beginning of Table ○ After id Go

Indexes:

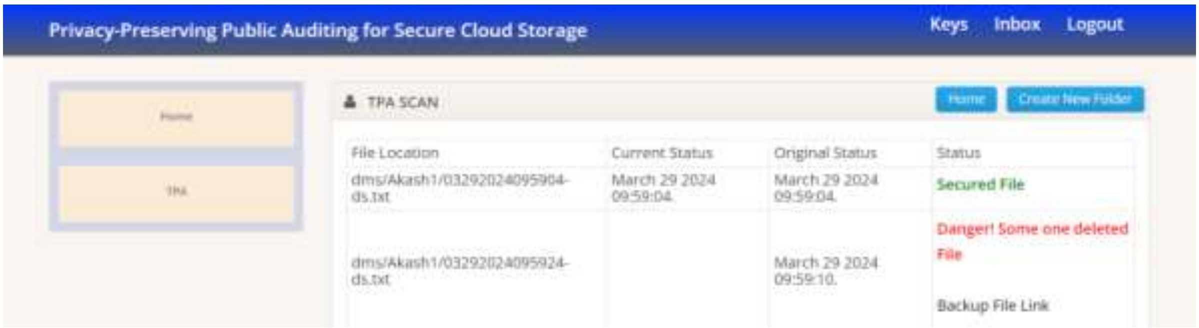
Keyname	Type	Unique	Packed	Field	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	64	A		

Create an index on 1 columns Go

+ Details...

Fig 9: Key Generation Session Table Structure

Figure shows key generation session table structure. It has four columns and they are: id, session id, public key, and private key.



File Location	Current Status	Original Status	Status
dms/Akash1/03292024095904-ds.txt	March 29 2024 09:59:04	March 29 2024 09:59:04.	Secured File
dms/Akash1/03292024095924-ds.txt		March 29 2024 09:59:10.	Danger! Some one deleted File Backup File Link

Fig 10: Data Recovery

V. CONCLUSION

In this paper, we introduce an innovative system aimed at enhancing the security of data storage in cloud computing while preserving user privacy. Our approach employs advanced techniques such as homomorphic linear authenticators and random masking to ensure that third-party auditors (TPAs) cannot access the actual content of data stored on cloud servers during the auditing process. This not only relieves cloud users from the burden of conducting time-consuming and potentially costly audits but also addresses concerns about potential data leaks. Moreover, recognizing that TPAs may need to handle multiple audit sessions simultaneously for different users' data files, we extend our privacy-preserving auditing protocol to support a multi-user setting. This allows TPAs to conduct multiple auditing tasks efficiently in batch mode, thereby improving overall system efficiency. Extensive analysis confirms the security and efficiency of our proposed schemes. Additionally, preliminary experiments conducted on an Amazon EC2 instance demonstrate the rapid performance of our design, both from the perspective of the cloud provider and the auditor. Looking ahead, we acknowledge the importance of fully implementing our mechanism on commercial public cloud platforms. Doing so will enable us to effectively manage very large-scale data and instill greater confidence among users in adopting cloud storage services. This represents a significant future extension of our work, which we believe will further bolster the widespread adoption of cloud technologies.

VI. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ’10, Mar. 2010.

[2] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” Technical Report UCB-EECS-2009-28, Univ. of California,Berkeley, Feb. 2009. WANG ET AL.: PRIVACY-PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STORAGE 373

[4] Cloud Security Alliance, “Top Threats to Cloud Computing,” http://www.cloudsecurityalliance.org, 2010.

[5] M. Arrington, “Gmail Disaster: Reports of Mass Email Deletions,” http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.

[6] J. Kincaid, “MediaMax/TheLinkup Closes Its Doors,” http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits-doors/, July 2008.

[7] Amazon.com, “Amazon s3 Availability Event: July 20, 2008,” http://status.aws.amazon.com/s3-20080720.html, July 2008.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011

[9] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D., 2007. Provable data possession at untrusted stores. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 598–609

[10] Koe, A.S.V., Lin, Y., 2019. Offline privacy preserving proxy re-encryption in mobile cloud computing. Pervasive Mob. Comput. 59, 101081.

[11] Li, Y., Yu, Y., Yang, B., Min, G., Wu, H., 2018. Privacy preserving cloud data auditing with efficient key update. Fut. Gen. Comput. Syst. 78, 789–798.

[12] Lu, X., Pan, Z., Xian, H., 2020. An efficient and secure data sharing scheme for mobile devices in cloud computing. J. Cloud Comput. 9 (1), 1–13.

[13] Mahmood, G.S., Huang, D.J., 2019. PSO-based steganography scheme using DWTSVD and cryptography techniques for cloud data confidentiality and integrity. J. Comput. 30 (6), 31–45