Enhancing Cloud Storage Security: Identity Management, Data Concealment, and Secure Sharing

N SUBRAMANYAM[1], POLUBOINA GEETHA[2]

[1]Assistant Professor,Dept of MCA, Audisankara college of Engineering and Technology (AUTONOMOUS),Gudur (M), Tirupati (Dt),AP

[2]PG Scholar, Dept of MCA,Audisankara college of Engineering and Technology (AUTONOMOUS)Gudur (M), Tirupati (Dt),AP

ABSTRACT_ In cloud computing, a secure storage system is a crucial component. Cloud clients use cloud auditing schemes to check the accuracy of cloud-stored data. However, regardless of how robust the auditing strategies may be, cloud auditing will fail if the auditing secret key is made available to the Cloud Service Provider. As a result, it is essential to keep auditing secret keys from being exposed, and even if this does happen, it must be minimized. Because they are based on Public Key Infrastructure, the current cloud auditing schemes that are extremely resilient to key exposure face difficulties with certificate management and verification. During data block integrity verification, these schemes also consume a significant amount of computation time. The Identity-based schemes don't use certificates at all, but they limit the damage caused by key exposure only in time periods before the key was exposed. Batch auditing is not supported by some of the key exposure resilient schemes. An Identity-based Provable Data Possession scheme is proposed in this paper. It safeguards Identity-based cloud storage auditing's security in time periods that are both earlier and later than the exposed key's time period. It additionally offers help for bunch examining. Investigation shows that the proposed plot is impervious to the supplant assault of the Cloud Specialist co-op, jam the information protection against the Outsider Examiner, and can productively check the rightness of information. During data block integrity verification, these schemes also consume a significant amount of computation time. The Identity-based schemes don't use certificates at all, but they limit the damage caused by key exposure only in time periods before the key was exposed. Batch auditing is not supported by some of the key exposure resilient schemes. An Identity-based Provable Data Possession scheme is proposed in this paper. It safeguards Identity-based cloud storage auditing's security in time periods both prior to and subsequent to the exposekey's time period.

1.INTRODUCTION

The rapid development of communications and networks in recent years has increased data transmission and exchange. Meanwhile, the demand for multimedia, such as video, pictures, and audio is increasing. Due to this important development, providing information technology (IT) services has become extremely costly to individuals and businesses. In this regard, Cloud computing is an efficient and good environment in terms of providing necessary IT services due to its economic advantages (Tian et al., 2019).

Cloud computing is a good experience with deep implications for changing the way enterprise uses IT. One of the key aspects of this model is that the data is focused or intended for cloud computing. From the viewpoint of users, involving information technology enterprises and individuals, remote data storage in the cloud paradigm in a flexible on-request method brings good advantages such as reduce the load on storage management, overall data access to different geographic positions, and decrease spending on devices, software, maintenance, etc. (Alrabea, 2020). Cloud storage is one of the basic technologies in the cloud paradigm. Many systems discussed it for low cost and high efficiency of cloud storage; therefore cloud data storage will transform data centres into a large-scale computing service. Of course, the fast growth of bandwidth to the network combined with trust and flexible connection of the network will make users enjoy high-quality cloud services (Ping et al., 2020). Cloud storage is dissimilar from traditional storage technologies. It affords large storage space for users and access to data through separate geographical locations. In other words, cloud users can easily access external data from any device connected to the network and connected to thecloud model anytime and anywhere

Despite the enormous benefits of the cloud model, there are also security challenges facing usersthrough their use of outsourced data. Since the management entities of the cloud service provider are separate, the users will relinquish control over their data. Thus, there are many reasons why data correctness on the cloud is at risk. First, cloud computing infrastructures face external and internal threats to data integrity, instances of service unavailable and security breaking of noticeable cloud computing services emerge from one interval to another Moreover, cloud service providers have many incentives to perform dishonestly to the status of cloud computing users concerning their external data

2.LITERATURE SURVEY

2.1.1 TITLE: Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage

ABSTRACT: Asha S; Punitha. K; Tanmay Joshi

AUTHORS: With the increase in the data growth, where data storage becomes difficult if the user wants to store it on a local drive, which is why many organizations and people prefer storing their data on a cloud storage. With accessibility of cloud storage, people can remotely use cloud storage and avail data storage. Remote data integrity has been suggested as a way to ensure the integrity of data stored in clouds. The health care system is one example of cloud storage, and the cloud file there may include sensitive data. This sensitive information should not be shared with others. One solution would be to encrypt the whole file to avoid sensitive data sharing, but then this way the file would be unusable to others. The method for implementing data sharing with sensitive information disguised in remote data integrity audits is one topic that hasn't been looked into yet. This technique does this by creating a sanitizer that will clean up data blocks that correspond to the sensitive information in the file and change those signatures into valid ones for the cleansed file. These signatures are utilised during the integrity auditing procedure to confirm the cleaned-up file. As a result, this scheme allows files to be shared with others, while also maintaining data security by sanitizing blocks of sensitive data, with the data integrity auditing still able to be executed efficiently without any problems. Identity-based cryptography, which the proposed solution is built on, makes complex certificate administration simple. The proposed method is efficient and secure, according to the performance analysis and security analysis.

2.1.2 TITLE: Identity-Based Public Auditing Scheme for Cloud Storage with Strong Key-Exposure Resilience

ABSTRACT: S. Mary Virgil Nithya

AUTHORS: Secured storage system is a critical component in cloud computing. Cloud clients use cloud auditing schemes to verify the integrity of data stored in the cloud. But with the exposure of the auditing secret key to the Cloud Service Provider, cloud auditing becomes unsuccessful, however strong the auditing schemes may be. Therefore, it is essential to prevent the exposure of auditing secret keys, and even if it happens, it is necessary to minimize the damage caused. The existing cloud auditing schemes that are strongly resilient to key exposure are based

on Public Key Infrastructure and so have challenges of certificate management/verification. These schemes also incur high computation time during integrity verification of the data blocks. The Identity-based schemes eliminate the usage of certificates but limit the damage due to key exposure, only in time periods earlier to the time period of the exposed key. Some of the key exposure resilient schemes do not provide support for batch auditing. In this paper, an Identity-based Provable Data Possession scheme is proposed. It protects the security of Identity-based cloud storage auditing in time periods both earlier and later to the time period of the exposed key. It also provides support for batch auditing. Analysis shows that the proposed scheme is resistant to the replace attack of the Cloud Service Provider, preserves the data privacy against the Third Party Auditor, and can efficiently verify the correctness of data.

2.1.3 TITLE: Empower Identity-Based Integrity Auditing And Information Distribution With

Confidential Data Defeat For Safety Cloud Storage

ABSTRACT: Dr D Nagaraju, Mrs R Bhavani, Kande Srinivas

AUTHORS: Users can use cloud storage services to remotely store their data and enable data sharing with others. Remote data integrity verification is advised in order to guarantee the accuracy of data saved in the cloud. Some prominent cloud storage platforms, like the electronic medical record system, may have files with sensitive data on them. Confidential information shouldn't be made available to others while sharing a cloud file. The entire shared file can be encrypted to protect sensitive information, but doing so prohibits others from accessing it. It is still unknown how sensitive data sharing with distant data integrity checks will be carried out. We recommend a remote data integrity verification method that implements the sharing of sensitive data hidden in this study to address this issue. This method uses a cleaner to make data block signatures valid for the file being processed while cleaning data blocks that correspond to sensitive data in the file. In the integrity check phase, these signatures are used to verify the correctness of the cleaned file. As a result, our method allows you to share and access a file stored in the cloud while sensitive data is masked, while you can efficiently perform remote data integrity checks.

3.PROPOSED SYSTEM

Far off information trustworthiness evaluating is proposed to ensure the uprightness of the information put away in the cloud. In some normal distributed

storage frameworks, for example, the electronic wellbeing records framework, the cloud document could contain some delicate data. The delicate data ought not be presented to others when the cloud document is shared. Encrypting the entire shared file will prevent other people from using it, but it will reveal the hidden sensitive information. The most effective method to acknowledge information imparting to delicate data concealing in far off information honesty evaluating still has not been investigated up to now. To resolve this issue, we propose a distant information respectability examining plan that acknowledges information offering to delicate data concealing in this paper. In this plan, a sanitizer is utilized to clean the information blocks relating to the delicate data of the record and changes these information blocks' marks into legitimate ones for the disinfected document. During the integrity auditing phase, these signatures are utilized to confirm the sanitized file's integrity. Accordingly, our plan makes the document put away in the cloud ready to be shared and utilized by others relying on the prerequisite that the delicate data is covered up, while the far off information trustworthiness reviewing is as yet ready to be proficiently executed

3.1 IMPLEMENTAION

Admin: Conduct a comprehensive analysis of existing cloud storage auditing systems to identify security Vulnerabilities and areas for improvement related to identity management, detection of hidden data, and secure sharing.

Initiator: Collaborate with the project team to design the architecture and functionalities of the initiator module, ensuring alignment with project goals and industry best practices.

Responder: Develop robust identity verification mechanisms within the responder module to authenticate users and ensure that only authorized individuals can respond to requests within the cloud storage environment.Implement algorithms and data analysis techniques to detect and address hidden data within the cloud storage system, enhancing transparency and compliance with data privacy regulations.

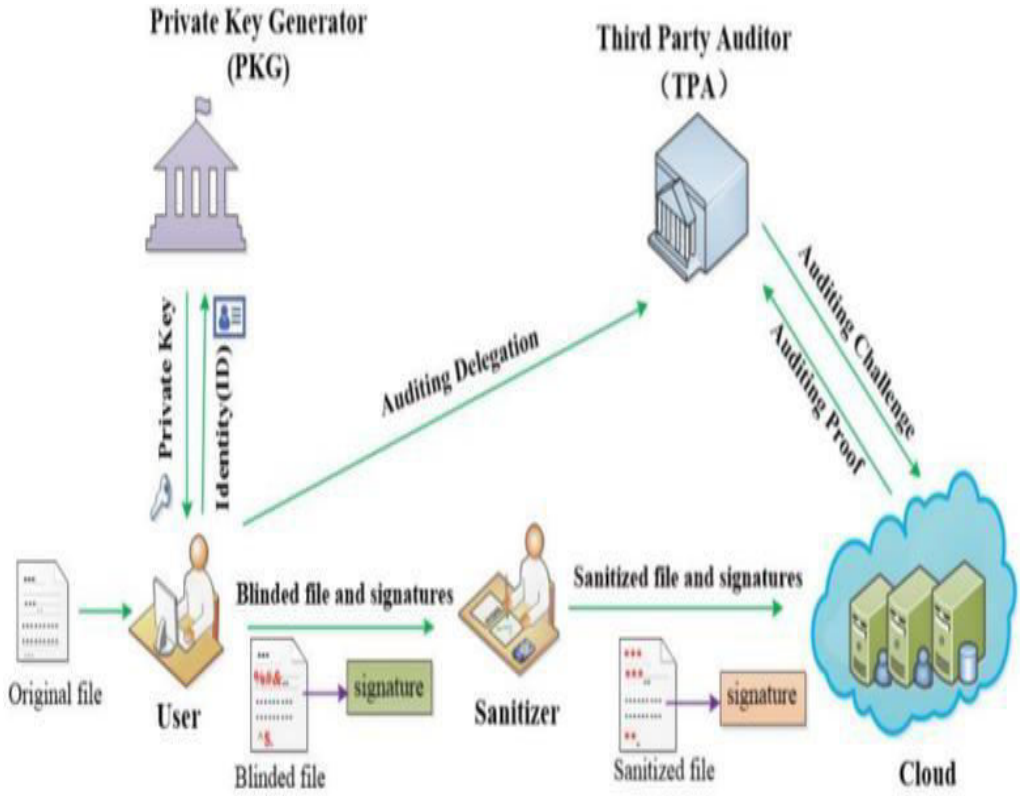

Fig 1:Architecture

4.RESULTS AND DISCUSSION

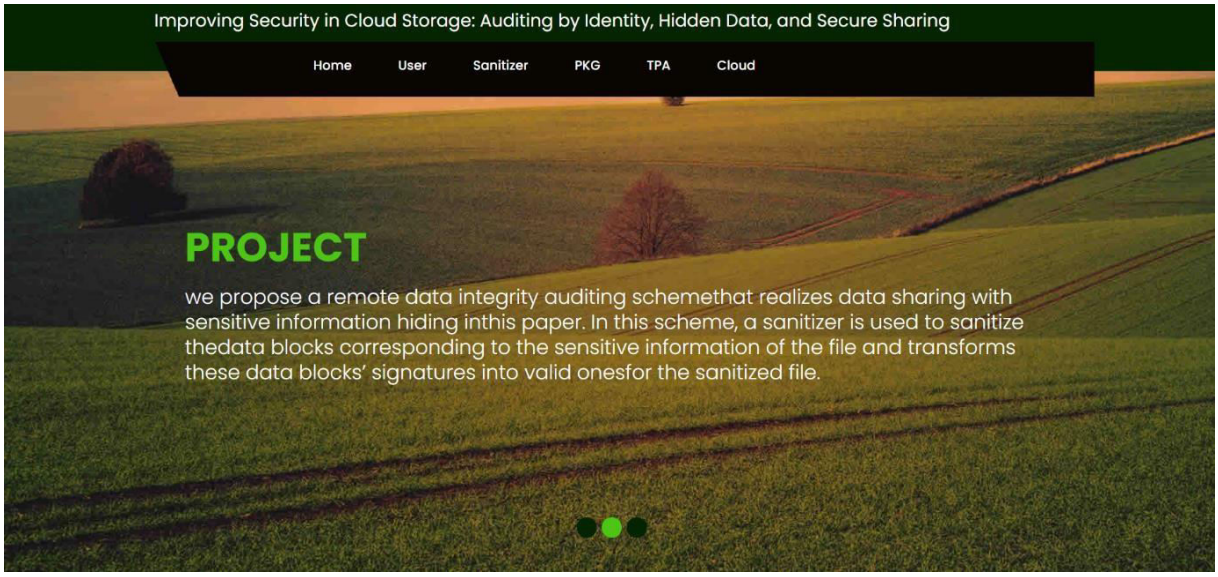

FIG-1 Home Screen

The term "Home screen" refers to the main or initial screen of an application or website that

users encounter upon opening the application or accessing the website. The home screen is essentiallythe starting point and often sets the tone for the rest of the user experience.

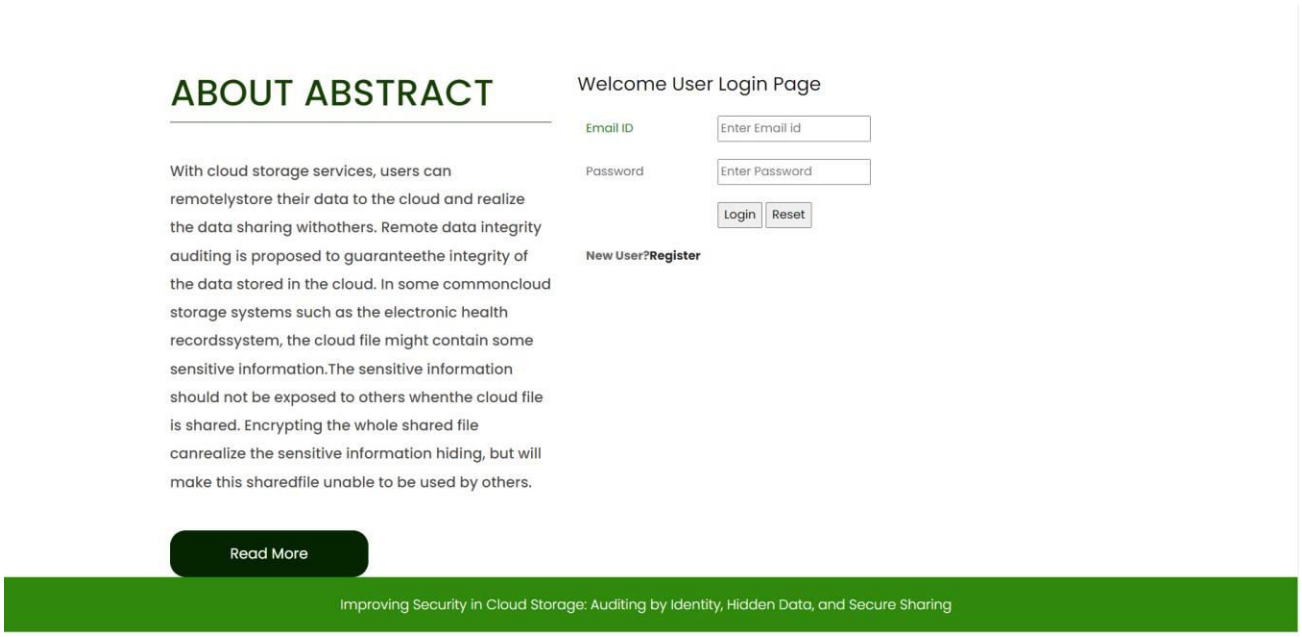

FIG 2 Registration page**:**A user registration page involves creating an interface where users can sign or register for your application or platform. Designing a user-friendly registration page is crucial for attractingusers and encouraging them to sign up for your project. Ensure that the registration process is intuitive, secure, and aligned with our project's objectives and branding.

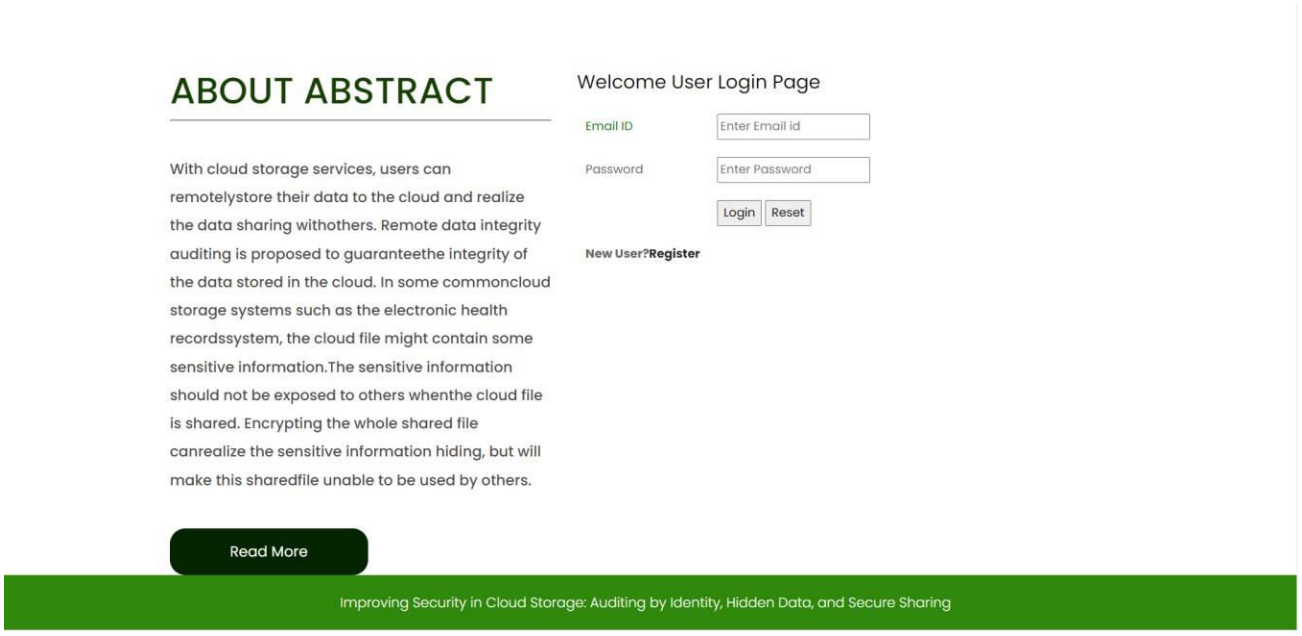

FIG-3 **login screen :An initiator/responder login screen is a type of login screen used in systems or applications that involve communication or interaction between two or more parties, often referred to as initiatorsand responders.**

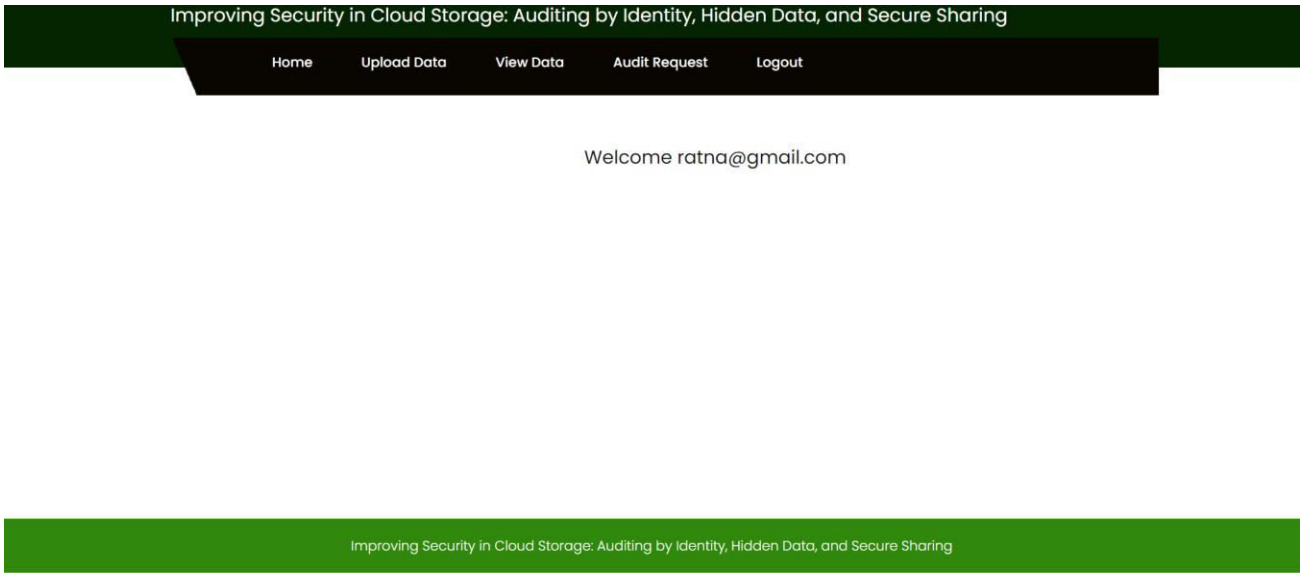

FIG-4 Admin Home Screen An Admin home screen requires careful consideration of the specific needs and responsibilities of administrators. Creating a user-friendly and efficient admin home screen is crucial foradministrators to effectively manage and oversee the system.

5.CONCLUSION

In this project, we proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding.

In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed.

The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency.

The need to preserve the integrity of data stored in the cloud rises with the growing demand for storage-as-a- service offering of cloud. So cloud storage auditing schemes are designed to verify the possession of cloud data but there are critical issues in these auditing schemes. This paper studies the auditing secret key

exposure problem in Identity-based cloud storage auditing schemes. Since exposure of secret key is undetectable, a better way to handle the key exposure problem is to minimize the damage caused by the exposed key. An Identity-basedstrong key-exposure resilient cloud auditing scheme using bilinear pairing is designed and implemented. The proposed scheme preserves the security of cloud auditing both before and after the key exposure by forward and backward security mechanism. Batch auditing is also incorporated into the scheme to ease the workload of the auditor. The scheme is provably secure using the computational Diffie–Hellman assumption in the random oracle model. Experimental results show that the proposed scheme is efficient in auditing the data block.

REFERENCES

1. Prescient & Strategic Intelligence, Global Enterprise Data Storage, Prescient & Strategic Intelligence, Noida, India, https://www.psmarketresearch.com/market-analysis/enterprise-data-storage-market.

2. A. D. Rayome, "69% of enterprises moving business-critical applications to the cloud," 2019, https://www.techrepublic.com/article/69-of-enterprises-moving-business-critical-applications-to-the-cloud/.
View at: Google Scholar

3. T. Singleton, "Why are so many 2018, https://datometry.com/blog/moving-to-the-cloud-survey-analysis/. View at: Google Scholar

4. T. Nikl and R. K. Chintalapudi, "8 common reasons why enterprises migrate to the cloud," 2018, https://cloud.google.com/blog/products/storage-data-transfer/8-common-reasons-why- enterprises-migrate-to-the-cloud.
View at: Google Scholar

5. Flexera, "Cloud computing trends," 2019, https://www.rightscale.com/blog/cloud-industry- insights/cloud-compu-ting-trends-2019-state-cloud-survey.
View at: Google Scholar

6. R. Oskoui, "5 Key cloud security challenges," 2018, https://www.cdnetworks.com/cloud-security/5-key-cloud-security-challenges/4208/.
View at: Google Scholar

7. G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07), pp. 598–610, Alexandria, VA, USA, November 2007.
View at: Publisher Site | Google Scholar

8. A. Juels and B. S. Kaliski, "PORs: proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07), pp. 584–597, New York, NY, USA, November 2007.
View at: Publisher Site | Google Scholar

9. H. Shachem and B. Waters, "Compact proofs of retrievability," in Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2008), pp. 90–107, Melbourne, Australia, December 2008.
View at: Google Scholar

AUTHOR'S PROFILE

Mr. N SUBRAMANYAM done M. tech from JNTU-Anantapur in 2022. He has been dedicated to the teaching field for the last 12 years. He is currently working as Assistant Professor at Audisankara College Engineering and Technology (AUTONOMOUS), Gudur, Tirupati (Dt), Andhra Pradesh .

POLUBOINA GEETHA is pursuing MCA from Audisankara College Engineering and Technology (AUTONOMOUS) GUDUR, affiliated to JNTUA in 2024, Andhra Pradesh.