Preserving Remote Data Integrity Verification Secure with Identity Based Authentication for A Designated Verifier

P.Bhanumathi[1], P.Deepthi[2], R.Jyosna Devi[3]
[1,2,3]*Assistant Professor, Department of MCA, Sree Venkateswara College of Engineering, Nellore, AP.*

Abstract: The approaches for remote data possession checking (RDPC) in the context of cloud-based computing are reviewed, with a focus on the distinctions between public and private verification mechanisms. Identified verifiers are crucial because they allow specific entities to verify data integrity while protecting data privacy. Yanet al. give an example of how existing RDPC systems typically overlook data privacy concerns in favor of public key infrastructure (PKI)-based authentication. To solve these shortcomings, future RDPC solutions should employ advanced cryptographic techniques to ensure secure verification processes that prioritize data privacy in cloud storage environments. These advancements aim to enhance the security and reliability of cloud-based data storage and verification systems by merging robust privacy measures with efficient integrity checks, in line with evolving privacy regulations and user preferences.

Keywords: Data dynamics, Identity-based Cryptography, Designated Verifier.

I. INTRODUCTION

In contemporary data outsourcing settings, it is imperative to ensure the integrity of remotely stored data. Conventional solutions provide either public or private verification, but do not allow for the specification of a chosen verifier. Yan et al. presented a strategy with designated verifiers, but they depended on a complex public key infrastructure and disregarded data privacy considerations. Our suggested solution uses identity-based techniques to overcome these drawbacks by enabling data owners to name particular verifiers while ensuring data privacy via random integer blinding. Using a Merkle hash tree structure allows you to update data dynamically without having to deal with complicated certificate management. This introduction highlights the need for our proposed identity-based remote data ownership checking mechanism with designated verifiers, emphasizing both practical efficiency and privacy preservation.

While other verifiers might not be able to perform this kind of duty, in many realistic circumstances the data owner might anticipate selecting a specific validator to validate data that has been outsourced. For example, a user has previously independently confirmed confidential data that was outsourced. However, he is not permitted to use the Internet or perform private verification while he is in combat. Here, he plans to select a trustworthy verifier to review the outsourced data. This introduction emphasizes the practical efficiency and privacy protection of our proposed identity-based remote data ownership checking system with designated verifiers.

Competitors may fabricate identities in order to validate information and acquire commercial data about the company. Since cloud storage may be far less expensive than maintaining data on personal devices, cloud storage has grown in popularity as a method of data storage for users, or data owners (DOs). The DOs can effortlessly exchange and access these outsourced data on various devices and locations while taking advantage of the services offered by cloud firms. But once they transfer the data to the cloud service provider (CSP), they also lose all control over it. Meanwhile, it is very possible to lose user data for the CSP for a variety of internal or external reason. For instance, the CSP might purposefully remove users' infrequently used data in order to free up space on its own, draw in additional customers, and increase revenue. Furthermore, cloud providers could experience hacker attacks, in which case customer data would be "passively" lost. But this creates new challenges. Generally speaking, the secret key should only be used for routine decryption and should not be utilized to change the ciphertext on a regular basis. To modify the shared data's ciphertext, the data provider needs to periodically carry out the download-decrypt

encrypt-upload process. With this technique, processing and communication costs are high for cloud users with limited processing and storage capacity.

In this work, we improve the RDPC system with the assigned verifier. In view of the complex certificate management procedures in PKI and the semi-trusted issue of the verifier, we propose a novel RDPC method. The principal contributions are as follows:

1. We develop an IBC-based RDPC system with a designated verifier in order to address the certificate management problem.
2. Our plan achieves data privacy. The CSP uses a random integer to blind the data integrity proof, ensuring that the verifier does not get any data content.
3. To fulfill the demands of quick data updates and facilitate dynamic data operations, our approach makes use of the Merkle hash tree (MHT).
4. We demonstrate the security of our technique and assess the processing and transmission expenses. In conclusion, our plan is more practical and effective based on the trial findings.

II. LITERATURE SURVEY

- The ID-based Remote Data Integrity Checking (ID-based RDIC) protocol was introduced by Yong Yu et al. (2016) as a means of simplifying key management and providing strong security for data integrity in cloud storage.
- The Identity-based Remote Data Integrity Checking for Cloud Storage approach was presented by Jigue Li et al. in 2020.It is suitable for real-world applications since it offers streamlined certificate administration and effective remote data integrity checks.
- Chang et al. [] first raised the related-key attack problem and developed a security model for identity-based signature methods. By demonstrating an intrinsic connection between identity-based network coding and identity-based evidence of retrievability, Chen and Chang improved the current structures for network coding and cloud storage.
- To ensure data ownership in untrusted clouds, Ateniese et al. (2007) proposed a proven data possession (PDP) technique.
- Jules et al. devised the proof of recoverability (POR) model [9], which guarantees the integrity of compromised data while allowing its restoration; nevertheless, the data owner is only allowed a limited number of data checks.

III. EXISTING METHOD

To enable remote data possession checking, or RDPC, in cloud computing, data must first be encrypted for confidentiality in the current technique before being uploaded to the cloud. To guarantee integrity and authenticity, a message authentication code (MAC) is calculated over the encrypted data. The cloud server generates a proof of possession in response to a verifier's challenge as part of a challenge-response protocol used for verification. Homomorphic encryption and other privacy-preserving techniques are used in designated verifier settings to identify specific verifiers and restrict access to the content during verification. Secure key management techniques are required for the safety of encryption keys, cloud-based data storage, and verification processes.

IV PROPOSED METHOD

We talk about improving a current system that checks the security of data stored in cloud computing settings. The prior system had certain problems because it was hard to administer and you could never be 100% sure who was checking the data. As a result, we generated new, improved data.In order to mitigate the challenges associated with handling PKI certificates and semi-trusted verifiers in cloud environments, the remote data possession checking (RDPC) technique adds a chosen verifier.

Using Identity-Based Cryptography (IBC) technology to build an RDPC system with a chosen verifier, this solution effectively addresses the certificate management issue that is present in typical PKI techniques. This is one of its key strengths. The data integrity proof is blinded with a random number by the cloud service provider (CSP) using a special technique that keeps the verifier from seeing the actual data content while doing integrity checks. Data privacy is thus guaranteed. Additionally, the method makes use of Merkle hash trees (MHT) to facilitate quick data updates and dynamic operations, which enhances the flexibility and efficiency of managing changing data sets. The technique's security and efficiency are proved through experimental results, and its performance is evaluated in terms of processing and communication costs. Overall, the recommended approach provides a practical and effective solution for remote data integrity verification in cloud environments by combining IBC, privacy-preserving techniques, and efficient data structures like MHT. As a result, the

verification process is more efficient, flexible, and secure.

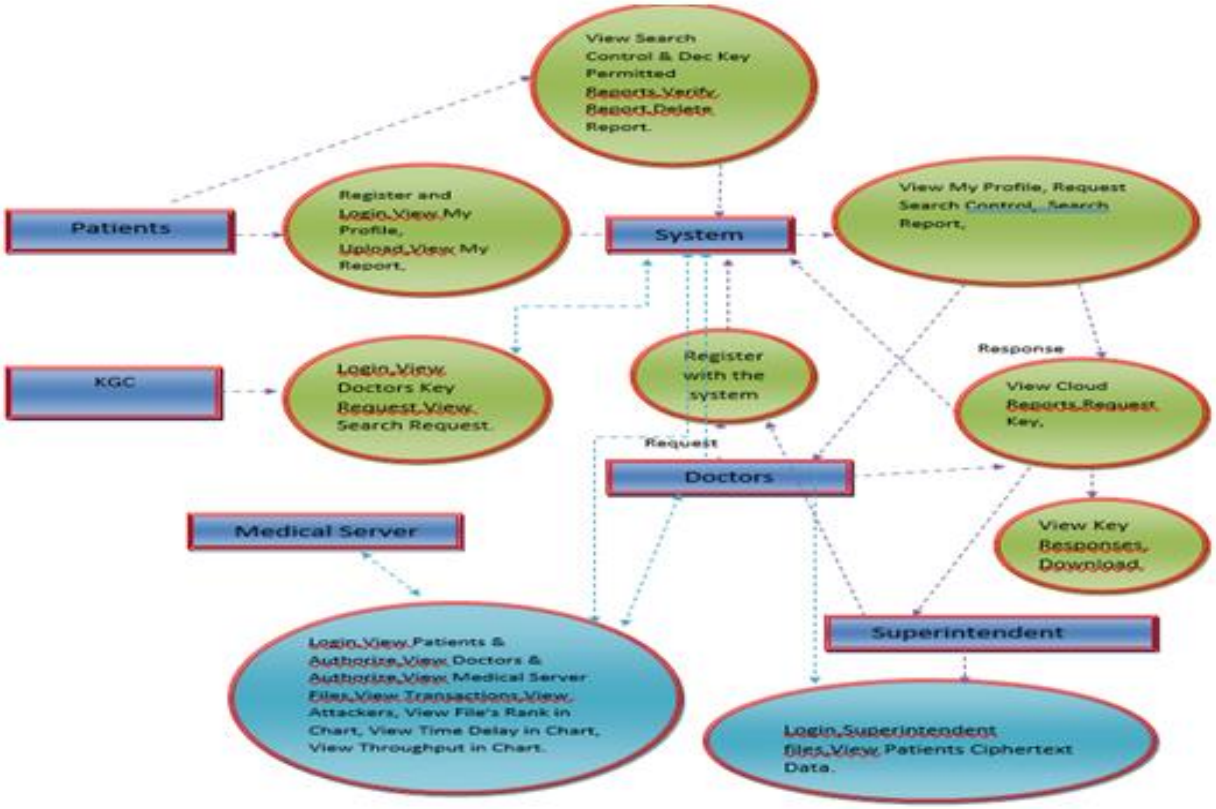

Fig 1: Data Flow diagram

This graphic shows a basic medical system with a focus on record keeping and patient-physician contact. Patients have the option to register and perhaps examine their medical profiles. Medical records and a list of patients are accessible to physicians. Patient data is likely stored on a central "Medical Server" in addition to acting as a communication hub. Probably for medical professionals, a "auth" process verifies user credentials before granting access to patient data. Furthermore, there is a "Superintendent" whose precise duties are unclear. The system offers a basic foundation for patient-doctor communication, but because of its peculiar lexicon and lack of details, it may be difficult to completely comprehend its potential.

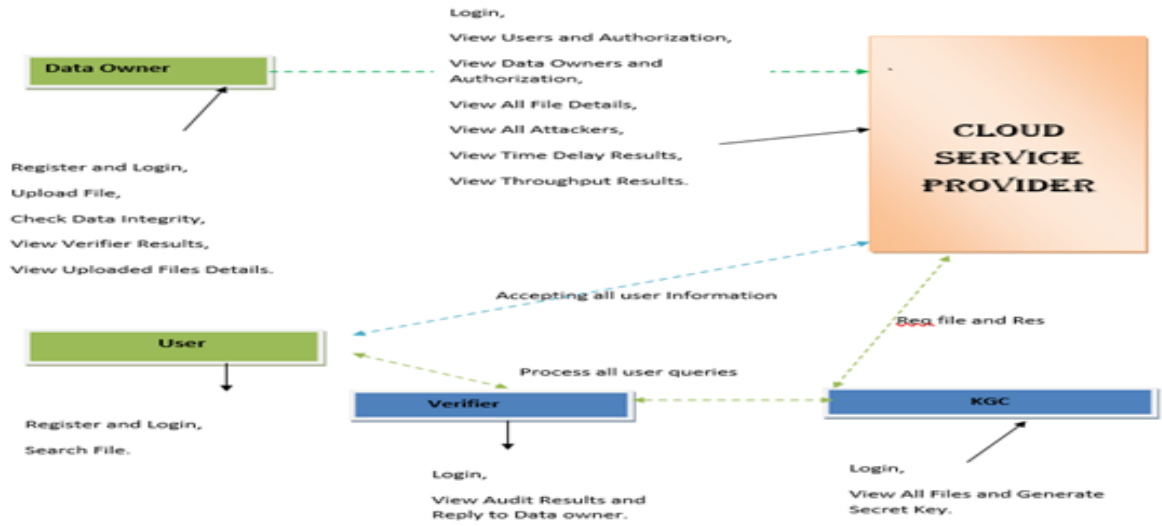

Fig 2: Architecture Diagram

A dual access control secure cloud storage system is demonstrated by this architecture. Guests have the ability to search for files, register, upload files, and log in. An alternate verifier in charge of access control audits can see logs and reply to users. The cloud service provider manages all user and data owner rights, logins, and access for all users, owners, and even attackers (perhaps illegal users). They are in charge of processing user data, file information, and system performance metrics. The cloud provider demonstrates a noteworthy two-step verification process to ensure data security, which involves verifying data integrity and cross-referencing the verifier's conclusions. This dual access technique adds an additional layer of protection for sensitive data hosted in the cloud.

Our suggested approach incorporates the suggested algorithms, including:

• Identity-Based Verification Setup: Establish system configurations and public/private key pairs for the chosen verifier, the data owner, and any additional parties involved in the verification process.

• Data Blinding Algorithm: Use a random integer blinding technique to mask the data integrity evidence before submitting it to the designated validator.

• Merkle Hash Tree Construction: Using the data blocks, create a Merkle hash tree to provide efficient verification and dynamic changes.

V. RESULTS

Fig 3:Homepage

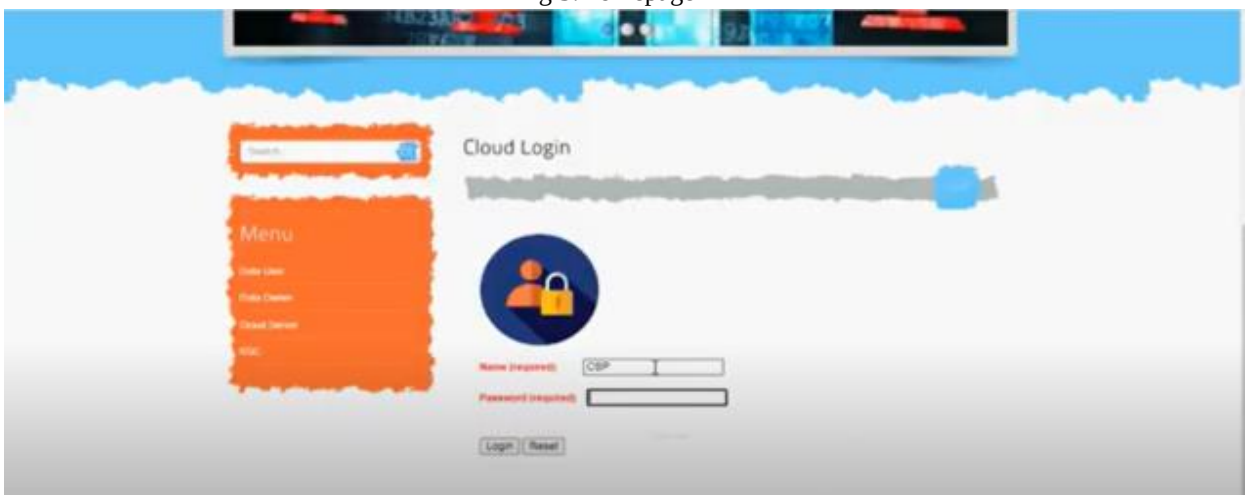

Fig 4: Registration Process

According to the figure 4, this is the login interface for the cloud service known as CRA. To indicate that the connection is secure, it employs a lock icon. The login and reset buttons are located beneath the lock icon, followed by menu options.

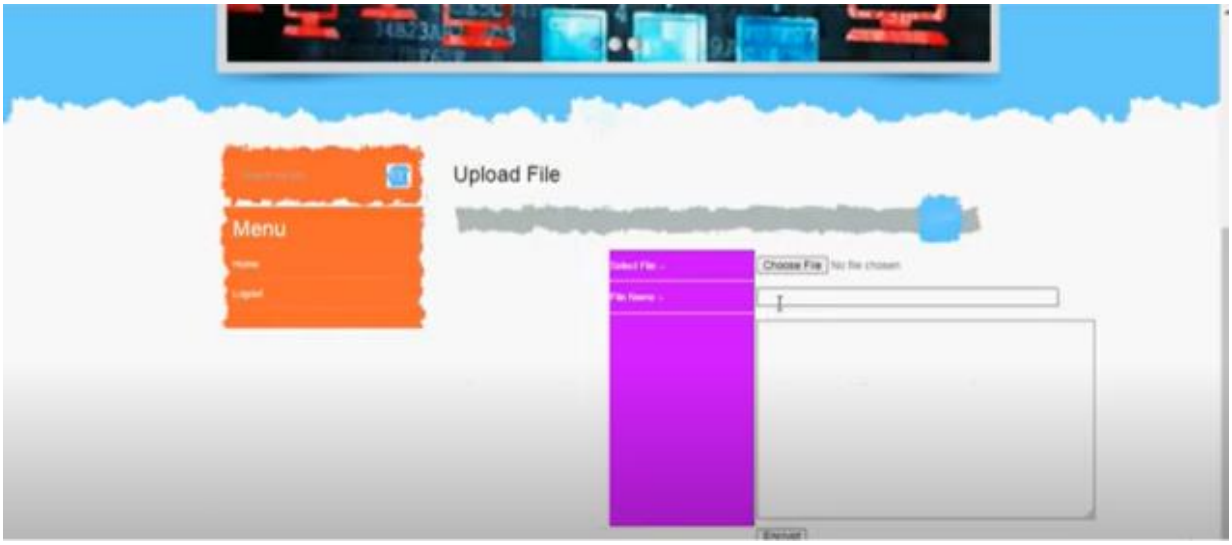

Fig 5: Uploading the data or File

This Figure 5 depicts that the files or data will be uploaded in this page to generate the secret keys

Fig 6: Generating the secret keys

This figure 6 depicts for generating the secret keys

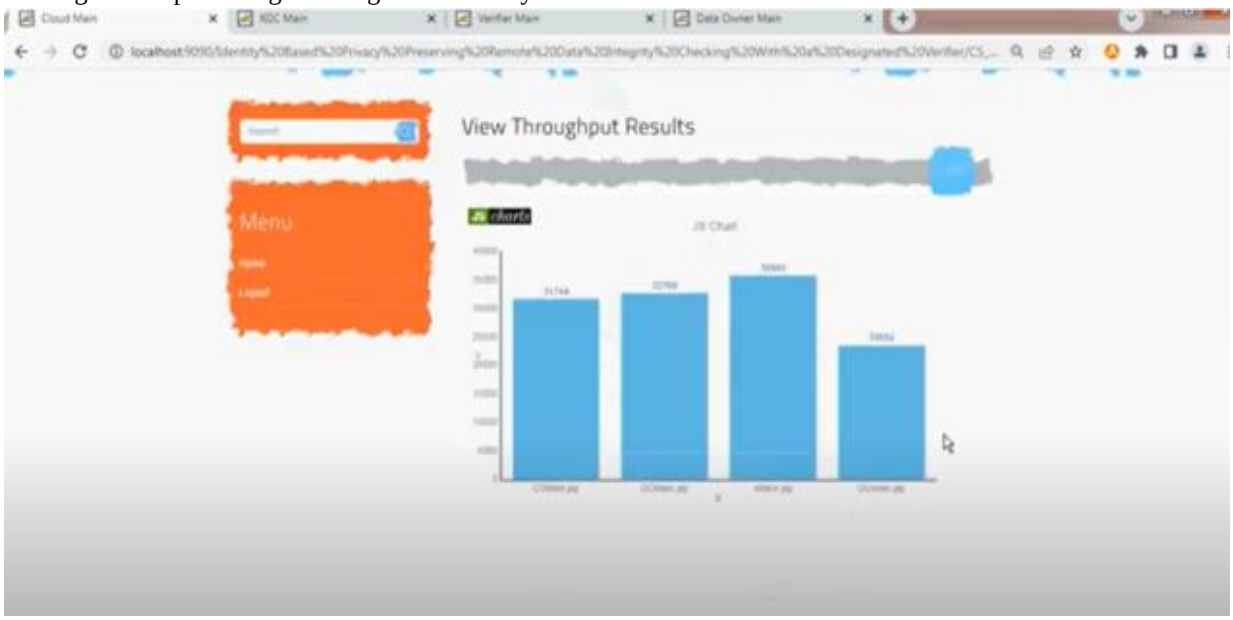

Fig 7: Final output/Results

VI CONCLUSION

In Conclusion to sum up, Yan et al.'s suggested technique offers a practical way to remotely verify data integrity while protecting privacy, using identity-based authentication for a selected validator. Through the use of identity-based encryption, the technique guarantees that integrity checks on the outsourced data may only be carried out by the designated verifier who possesses a designated identity. This strategy is in line with real-world situations where data owners need to know that their data can be accessed and verified for accuracy by only designated, reliable parties without jeopardizing their privacy Even while designated verification is heavily emphasized in the strategy, more work needs to be done to protect personal data, particularly in cloud computing environments. Future studies should examine methods to improve data integrity verification and privacy protection in order to meet the changing security requirements for cloud-based data storage.

REFERENCE

[1] M. Armbrust, A. Fox, R. Grif_the, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, ``A view of cloud computing," *Commun ACM*, vol. 53, no. 4, pp. 50_58, Apr. 2010.

[2] D. Zissis and D. Lekkas, ``Addressing cloud computing security issues," *Future Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583_592, Mar. 2012.

[3] J. Lu, F. Nan, Y. Huang, C.-C. Chang, Y. Du, and H. Tian, ``Privacy- preserving public auditing for secure data storage in fog-to-cloud comput-ing," *J. Netw. Comput. Appl.*, vol. 127, pp. 59_69, Dec. 2018.

[4] Y. Deswarte, J.-J. Quisquater, and A. Saidane, ``Remote integrity check-ing," in *Proc. Work. Conf. Integrity Internal Control Inf. Syst.*, Cham, Switzerland: Springer, 2003, pp. 1_11.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ``Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 598_609.*Privacy*. Berlin, Germany, Springer, 2015, pp. 377_394.

[6]The article "Panda: Public auditing for shared data with efficient user revocation in the cloud" was published in January/February 2015 in IEEE Trans. Serv.Comput.

[7] In Proc. Australas. Conf. Inf. Secur., Y. Feng, Y. Mu, G. Yang, and J. K. Liu present "A new public remote integrity checking scheme with user privacy."

[8] H. Yan, J. Li, and Y. Zhang, "Remote data checking in cloud storage using a designated verifier," IEEE Syst. J., June 2020; vol. 14, no. 2, pp. 1788_1797.

[9] Pors: Proofs of retrievability for big _les, A. Juels and B. S. Kaliski, Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584_597.

[10] Compact proofs of retrievability, by H. Shacham and B. Waters, Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., Berlin, Germany, Springer, 2008, pp. 90_107.

[11]. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, " Cryptography goes to the cloud," in Proc. Secure and Trust Computing, Data Management, and Applicat. (STA 2011 Workshops), 2011, pp. 190–197.

[12]. G. Ateniese et al., " Provable data possession at untrusted stores," in Proc. 14th ACM conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

[13].G. Ateniese, A. Faonio, and S. Kamara, " Leakage-resilient identification schemes from zero-knowledge proofs of storage," in Proc. IMA Int. Conf. Cryptogr. Coding, 2015, pp. 311–328.