**ENABLING IDENTITY-BASED INTEGRITY AUDITING AND DATA SHARING WITH SENSITIVE INFORMATION HIDING FOR SECURE CLOUD STORAGE**

**Mr. Swanand Sabale1, Miss. Bhoomi Pawar2, Mr. Nayan Nighot3,Prof. Miss. Pawar. T. S4**

1Student, Computer Engineering, SPIT Polytechnic, Kurund, Ahilyanagar, Maharashtra, India

 2Student, Computer Engineering, SPIT Polytechnic, Kurund, Ahilyanagar, Maharashtra, India

 3Student, Computer Engineering, SPIT Polytechnic, Kurund, Ahilyanagar, Maharashtra, India

Guide, Department Computer Engineering, SPIT Polytechnic, Kurund, Ahilyanagar, Maharashtra, India

**1. ABSTRACT**

 The main goal of our project is to create a mobile application that allows users to remotely

save their data on the cloud and share it with others for auditing and data sharing via cloud storage services. To ensure the integrity of the data saved in the cloud, remote data integrity auditing is suggested. Cloud files may contain sensitive data in certain popular cloud storage services. Sensitive information can be hidden by encrypting the entire shared file, but doing so will prevent others from using it. In this work, we suggest a remote document reference ID that automatically transforms into a QR code. Users only need to scan the module to obtain the specific document integrity, which enable data exchange while concealing important information.

 With the help of cloud storage services, customers can share their data with others and store remotely. To ensure the integrity of the data saved in the cloud, remote data integrity auditing is suggested. The cloud file may include sensitive data in certain popular cloud storage systems, including the Electronic Health Records (EHRs) system. Sharing the cloud file should protect the private data from prying eyes. Sensitive information can be hidden by encrypting the entire shared file, but doing so will prevent others from using it. Up until now, no research has been done on how to implement data sharing while concealing sensitive information in remote data integrity audits

**Keywords:** Cloud, Concealing, Mobile Application, Data Integrity, Encrypting, Electronic Health Records**.**

**2. INTRODUCTION**

 New companies are newly formed entities that compete for market share. These components are typically constructed based on brilliant ideas and grow to be successful. The writing of administration, connection, and commercial speculations details these wonders. However, there isn't a clear picture of these compounds available. This essay aims to comprehend the challenges they would face and to conceptualize the marvel, or startup. The report concludes with some concluding remarks after examining the existence cycle and the challenges. This study looks for a respectable percentage of new business execution and then uses several business procedure measurements to clarify this metric. Clients find it quite burdensome to retain the vast amount of information locally due to its delicate development. As a result, more and more organizations and individuals are choosing to store their data on the cloud.

**3. METHODOLOGY**

 One approach for approving current, convenient, on-demand network access to a common pool of reconfigurable computer resources may be cloud computing. Interactions between its subparts (i.e., Clouds) and among stakeholders (i.e., consumers and Cloud providers) are complex because, as an associate degree puts it, Cloud may be a massive scale distributed and interconnected automatic data processing system. Applications and knowledge are available to and shared by a wide cluster of cross-platform and cross-enterprise users in an inter-cloud, where computing resources managed by many cloud providers are combined to service numerous clients. In summary, cloud resource pooling and sharing entails 1) mapping and arranging shared resources through collaboration among Clouds, 2) combining resources through coordination, and 3) negotiating contracts between Clouds and their clients as well as between Clouds.

 TESTING UNITS:

Planning test cases that confirm that the internal program logic is operating correctly and that program input produces legitimate outputs is known as unit checking. The internal code flow and all call branches should be legitimate. It involves testing the application's individual code units. Prior to integration, it is completed after a personal unit is finished. This may be an intrusive structural test that relies on construction knowledge. Unit checks examine a specific business method, application, and/or system configuration by performing basic tests at the part level. Unit tests ensure that each different path of a business procedure comprises inputs and expected results that are clearly defined and operates accurately to the stated specifications.

TESTING FOR INTEGRATION:

The progressive integration testing of two or more integrated code components on a single platform to identify errors brought on by interface flaws is known as code integration testing.

Combination checks are used to see that code applications or portions, such as code during a code or corporate code applications, move without errors.

TESTING FOR ACCEPTANCE:

Any project may benefit greatly from user acceptance testing, which requires the top user's active engagement. It also guarantees that the system satisfies the practical requirements.

Knowledge acceptance testing Synchronization: After the packets are received by the destination node, the sender node will receive the acknowledgements.

Only when there is a route request in need is the route add procedure finished.

The cache update method uses a mechanical process to finish the standing of nodes' data.

CONSTRUCT THE TEST PLAN:

Every project has units that will be carried out in a methodical manner. After that, a testing plan is implemented for each of these units. Unit testing aids in locating possible defects in each component so that the problematic element can be identified and fixed.

FAMEWORK:

Five distinct components are included in the system model: the user, the cloud, the sanitizer, the Private Key Generator (PKG), and the Third-Party Auditor (TPA).

1. Cloud: The user can store a vast amount of data in the cloud. Users can share their data with others and upload it to the cloud using the cloud storage service.
2. User: The user belongs to a company that has a lot of files that need to be kept on cloud servers.
3. Sanitizer: The sanitizer is responsible for sanitizing the data blocks that correspond to the sensitive information (both personal and organizational sensitive information) in the file, changing the signatures of these data blocks to ones that are appropriate for the sanitized file, and uploading the sanitized file to the cloud along with the corresponding signatures.

(4) PKG: Other entities have faith in the PKG. It is in charge of creating the user's private key and system public parameters based on his identity ID.

(5) TPA: A public verifier is the TPA. On behalf of users, it is responsible for confirming the accuracy of the data kept in the cloud.

 

 Fig.1. The system model

**4. MODELING AND ANALYSIS**

 The audit's data. The results of an associate auditor's audit of an organization's accounts or examination of its major financial statements are usually documented in a report or assembled in a methodical fashion.

 However, due to inevitable programming errors, equipment malfunctions, and human error, the data stored in the cloud may be tampered with or deleted. within the cloud Many remote information respectability examination plans have been presented with the ultimate purpose of determining whether the data is stored in the cloud efficiently. Before moving them to the cloud, the information owner must first create markings for information obstructions in remote information honesty review plans. certain marks are used to show that the cloud actually has certain informational barriers during the reliability assessment phase.

 And then the data stored in the cloud is frequently shared among various clients in a variety of distributed storage apps, such as iCloud, Dropbox, and Google Drive. One of the most fundamental features of distributed storage is information sharing, which enables different clients to share their information with others. In any event, certain sensitive information may be stored in these shared files stored on the cloud. For instance, Electronic Health Records (EHRs) stored on the cloud typically include sensitive information from the healing center as well as company auditing (company name, phone number, ID number, etc.).

 In this work, we suggest a remote document reference ID that automatically transforms into a QR code. Users only need to scan the module to obtain the specific document integrity, which enables data exchange while concealing important information.

**5. RESULTS AND DISCUSSION**

* **Performance Testing**:
Assess the encryption time, retrieval speed, and audit query efficiency.
* **Security Evaluation**:
Test the robustness of the system against threats like unauthorized access and tampering.
* **Scalability Analysis**:
Evaluate system performance as the number of users and data volume increases.
* **Usability Evaluation**:
Test the user-friendliness of the system, focusing on ease of use for data sharing and auditing.
* **Interplay of Integrity and Privacy**: The paper likely discusses how identity-based integrity auditing can be combined with privacy-preserving techniques to allow secure data sharing in the cloud. While integrity auditing ensures that actions are verifiable and transparent, privacy mechanisms such as sensitive information hiding ensure that data is protected from unauthorized access.
* **Cryptographic Approaches**: The use of identity-based encryption, zero-knowledge proofs, and other cryptographic methods can play a critical role in balancing the trade-off between security and privacy in cloud systems.
* **Future Directions**: The paper might conclude with potential future directions for research and development in secure cloud computing, including the evolution of privacy-preserving cryptographic methods, the improvement of auditing and monitoring tools, and the integration of new technologies such as blockchain for secure data sharing and accountability.

In summary, the integration of identity-based integrity auditing with sensitive information hiding in the cloud aims to strike a balance between ensuring the confidentiality of sensitive data and maintaining the integrity of user actions and system logs. This combination can greatly enhance the overall security of cloud environments, although it comes with challenges that need to be addressed through novel approaches in cryptography, access control, and auditing techniques.Top of Form

Bottom of Form

**6. CONCLUSION**

 The user can easily outsource the file to unreliable proxy servers with a distributed data storage architecture. Determine which types of distributed data storage schemes are based on safe distributed data storage schemes.where users are recognized by their identities and are able to communicate without requiring the public key certificate to be verified. For safe cloud storage, we suggested an identity-based data integrity auditing system that allows data exchange while concealing sensitive information.

 According to our plan, the cloud-stored file can beshared and utilized by others as long as the file's sensitive data is safeguarded. In addition, remote data integrity audits can still be carried out effectively. The experimental analysis and security proof show that the suggested strategy achieves the desired efficiency and security.

**7. ACKNOWLEDGEMENTS**

 We would like to express my sincere gratitude to everyone who has supported and guided me throughout the development of this research project, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage."

First and foremost, we would like to extend my deepest thanks to my supervisor, [Supervisor's Name], for their invaluable guidance, patience, and constant encouragement throughout the course of this research. Their expert advice, constructive feedback, and thoughtful suggestions have greatly enhanced the quality of this work.

 we would also like to thank the faculty members and staff at [Institution's Name] for providing the resources, tools, and support necessary to carry out this research. Their assistance has been instrumental in the successful completion of this project.

 My heartfelt thanks go to my friends, colleagues, and fellow researchers who contributed their ideas, provided constructive criticism, and shared their insights during various stages of the research. Your support and collaboration have been greatly appreciated.

We are also deeply grateful to my family for their unwavering support and understanding throughout this process. Their encouragement and belief in my abilities have been a constant source of motivation.

Finally, we could like to acknowledge all the researchers, authors, and developers whose work I have referenced in this study. Their contributions have been essential in shaping the direction of my research.

**7. REFERENCES**

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp. 598–609.

[3] 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, ser. CCS ’07, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[5] ISO/IEC 15420:2009. Information technology - Automatic identification and data capture techniques - EAN/UPC bar code symbologyspecification. 2009.

[6] ISO/IEC 16022:2006. Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification. 2006.

[7] ISO/IEC 18004:2000. Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code. 2000.

[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, “Light-weight and privacy- preserving secure cloud auditing scheme for group users via the third-party medium,” Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.

[9] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.