



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage

Rajanala Krishna Teja, Peddapally Monish, Bathula Bhargav Reddy, Y. Ashwini

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Student, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Assistant Professor, Department of Computer Science Engineering, Anurag University, Hyderabad, Telangana, India

Abstract: Cloud computing is an emergent paradigm to provide reliable and resilient infrastructure enabling the users (data owners) to store their data and the data consumers (users) can access the data from cloud servers. This paradigm reduces storage and maintenance cost of the data owner. At the same time, the data owner loses the physical control and possession of data which leads to many security risks. Therefore, auditing service to check data integrity in the cloud is essential. This issue has become a challenge as the possession of data needs to be verified while maintaining the privacy. To address these issues this work proposes a secure and efficient privacy preserving provable data possession (SEPDP). Further, we extend SEPDP to support multiple owners, data dynamics and batch verification. The most attractive feature of this scheme is that the auditor can verify the possession of data with low computational overhead.

KEYWORDS: Data privacy, Cloud Computing, Data integrity, MySQL

I. LITERATURE SURVEY

K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. In this paper, we investigate this kind of problem and give an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, we introduce some existing auditing schemes and analyze them in terms of security and performance. Finally, some challenging issues are introduced in the design of efficient auditing protocol for data storage in cloud computing.

B. Wang, B. Li, H. Li, and F. Li, “Certificateless public auditing for data integrity in the cloud,” in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–144.

Due to the existence of security threats in the cloud, many mechanisms have been proposed to allow a user to audit data integrity with the public key of the data owner before utilizing cloud data. The correctness of choosing the right public key in previous mechanisms depends on the security of Public Key Infrastructure (PKI) and certificates. Although traditional PKI has been widely used in the construction of public key cryptography, it still faces many security risks, especially in the aspect of managing certificates. In this paper, we design a certificateless public auditing mechanism to eliminate the security risks introduced by PKI in previous solutions. Specifically, with our mechanism, a public verifier does not need to manage certificates to choose the right public key for the auditing. Instead, the auditing can be operated with the assistance of the data owner's identity, such as her name or email address, which can ensure the right public key is used. Meanwhile, this public verifier is still able to audit data integrity without retrieving the entire data from the cloud as previous solutions. To the best of our knowledge, it is the first certificateless public auditing mechanism for verifying data integrity in the cloud. Our theoretical analyses prove that our mechanism is correct and secure, and our experimental results show that our mechanism is able to audit the integrity of data in the cloud efficiently.

C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in *Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010*, pp. 1–9.

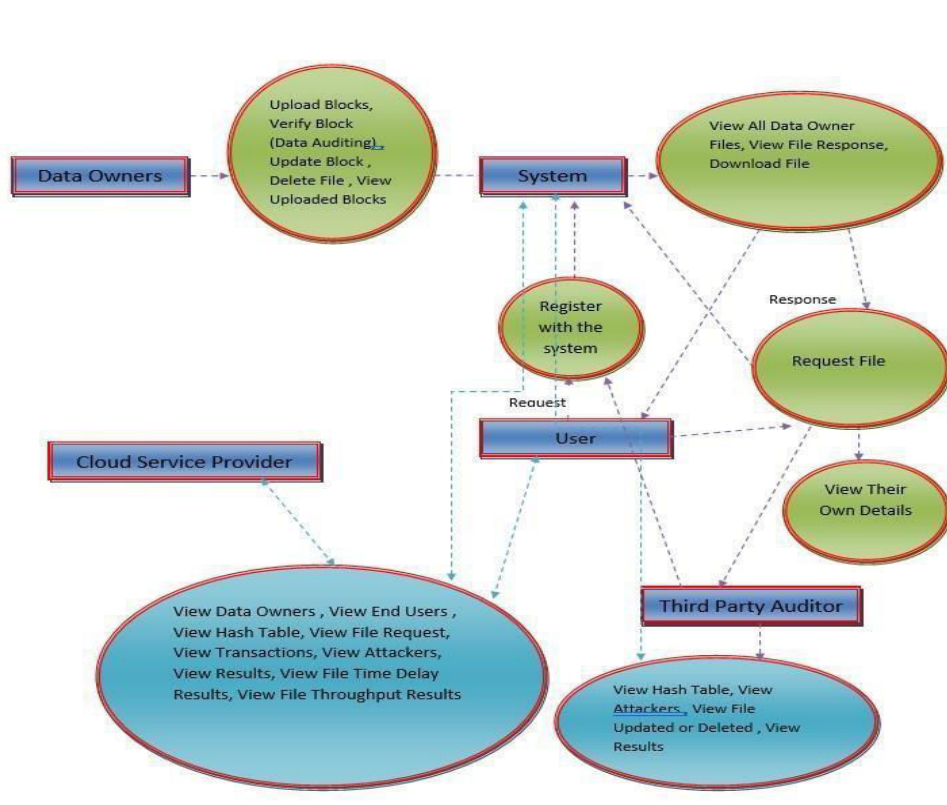
Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

II. METHODOLOGY AND APPROACH

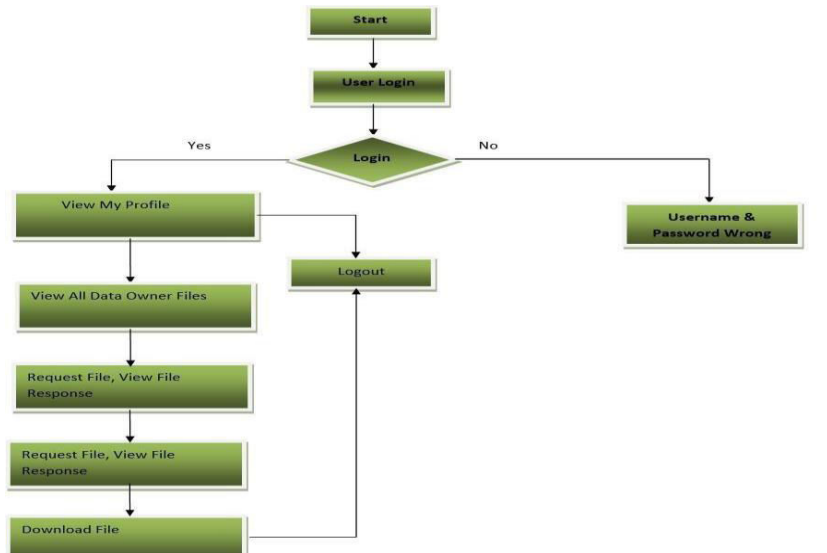
In the proposed work, the system proposes a secure and efficient privacy preserving provable data possession scheme (SEPD) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPD is that it does not use any intensive computation like pairing based operation.

Further, the system extends SEPD to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP. The system evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms.

The system observes that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPD is efficient and suitable to implement the verification at the low powered devices.



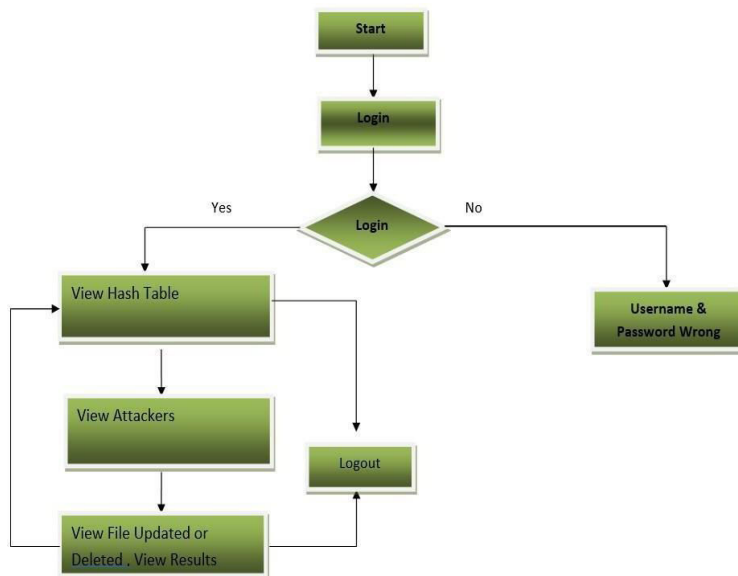
Modules User



In this module, he logs in by using his/her user name and password. After Login receiver will perform operations like View All Data Owner Files, Request File, View File Response, Download File

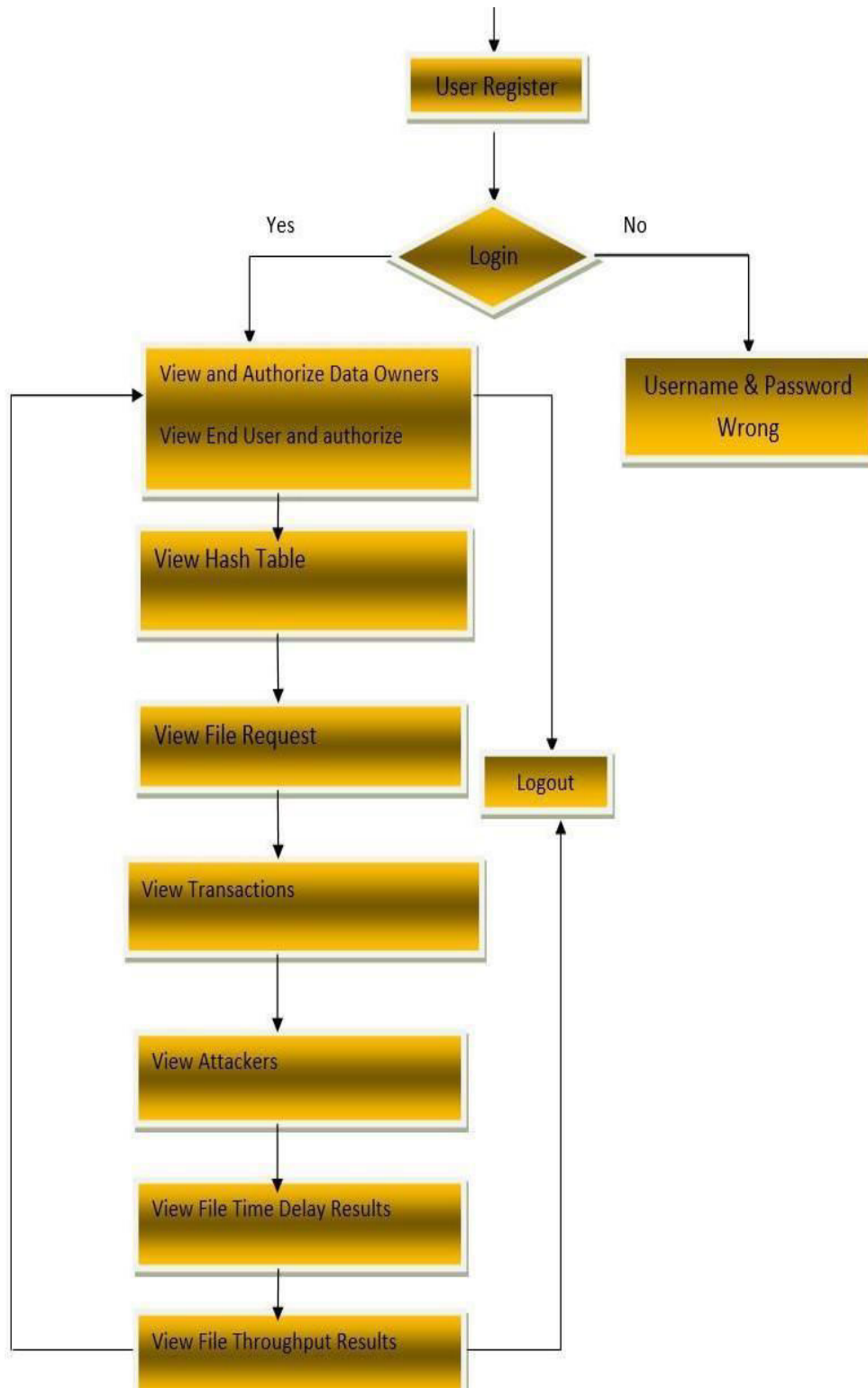
Third Party Auditor

In this module, the sector can do following operations View Hash Table, View Attackers , View File Updated or Deleted , View Results



Cloud Service Provider

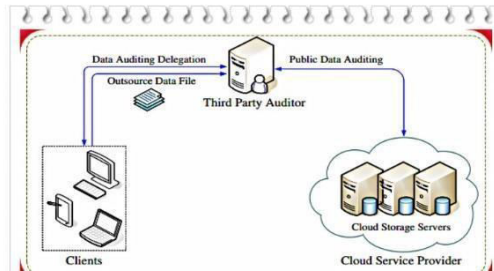
The Service Provider manages a server to provide data storage service and can also do the following operations such as View Data Owners , View End Users , View Hash Table, View File Request, View Transactions, View Attackers, View Results, View File Time Delay Results, View File Throughput Results





III. RESULTS AND DECLARATION

Here you can see the website after redirecting to the web browser Home Screen



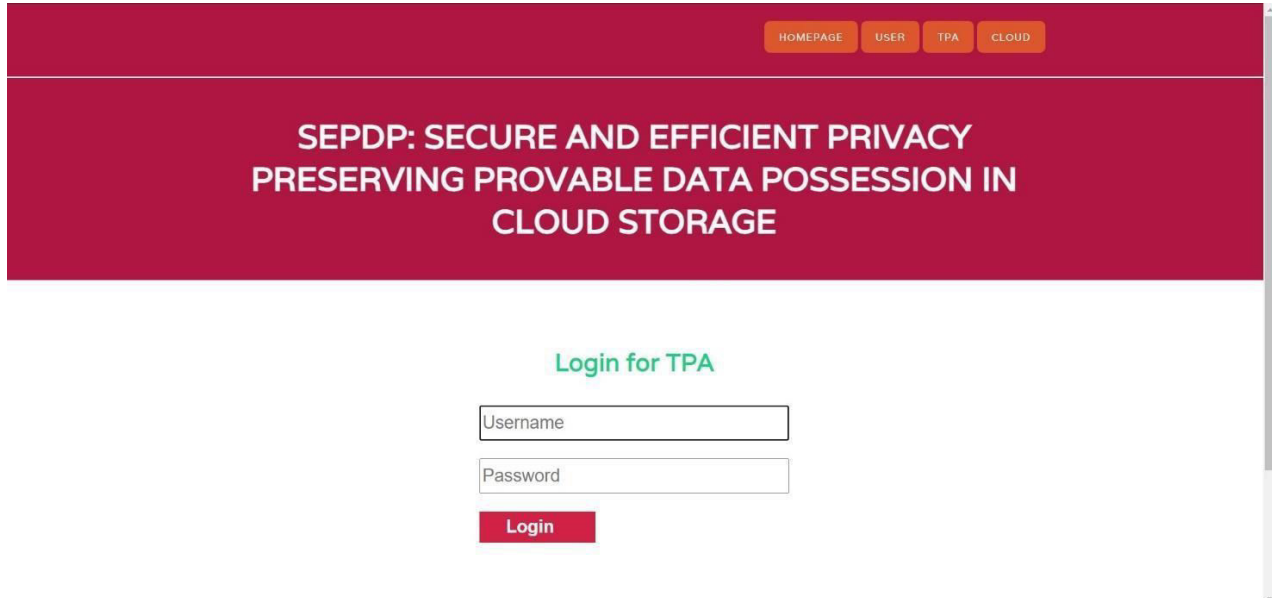
User Registration Verification for User



Your Data

S.No	File Id	Email	Status	Date
1	2	kittu@gmail.com	Data Verified	27/03/2024 06:25:35
2	2	kittu@gmail.com	Data Verified	28/03/2024 12:44:11

TPA Login



HOMEPAGE USER TPA CLOUD

**SEDPD: SECURE AND EFFICIENT PRIVACY
PRESERVING PROVABLE DATA POSSESSION IN
CLOUD STORAGE**

Login for TPA

Username

Password

Login

IV. CONCLUSION

In this paper, privacy preserving provable data possession scheme (named SEDPD) for untrusted and outsourced storage system is presented. Further, SEDPD is extended to support dynamic data updation by multiple owners and batch auditing. Security of the scheme is analyzed and showed that SEDPD protects data privacy from TPA while infeasible for CSP to forge the response without storing the appropriate blocks. The most appealing features of the proposed scheme is to support all the important features including blockless verification, privacy preserving, batch auditing and data dynamics with lesser computation overhead.

REFERENCES

1. K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.
2. B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in *Proceedings IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 136–144.
3. H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proceedings of 14th ASIACRYPT*, 2008, pp. 90–107.
4. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM)*, 2010, pp. 1–9.
5. L. Yuchuan, F. Shaojing, X. Ming, and W. Dongsheng, "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage," *China Communications*, vol. 11, no. 11, pp. 114–124, 2014.
6. B. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 485–497, 2015.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details