**USING CLOUD STORAGE, SEPDP STANDS FOR SECURE AND EFFICIENT PROVABLE DATA POSSESSION**

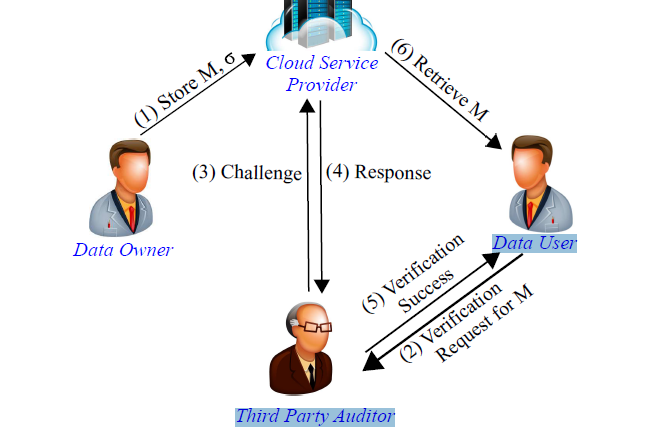
**ABSTRACT:-**

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.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * One uses pseudo-random function (PRF) which fails to provide public verifiability, while the other one uses boneh–lynn–shacham (BLS) signatures. * Both the schemes support blockless verification but fail to provide privacy of the DO’s data. * At the same time, the data owner loses the physical control and possession of data which leads to many security risks. | * In this work, we propose a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. * We extend SEPDP to support multiple data owners, batch auditing, and dynamic data operations. * We observe 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 SEPDP is efficient and suitable to implement the verification at the low powered devices |
| **EXISTING ALGORITHM**  Third party auditor (TPA). | **PROPOSED ALGORITHM:-**  secure and efficient privacy preserving provable data possession (SEPDP) |
| **ALGORITHM DEFINITION:-**  Therefore, the system consists of a third party auditor (TPA) to verify the integrity of outsourced data. Initially, DO shares a secret key with TPA through a secure channel using any standard technique like SSL/TLS. Every block of the outsourced data (mi) is tagged with a signature computed using the private key of DO. In the auditing phase, TPA sends a challenge to CSP and CSP returns a response to proof possession of the data. Thus, the public auditing schemes are a kind of challenge-response protocol. | **ALGORITHM DEFINITION:-**  In this section, we present the proposed secure and efficient data possession scheme (SEPDP). SEPDP achieves all the design goals discussed in previous section. SEPDP consists of three phases, namely, key generation phase, signature generation phase, and audit phase. The operations of these phases are depicted in and discussed below. For the sake of simplicity, we describe the scheme with a single DO and extend the scheme to support multiple .Notations used in this work are stated in are system wide parameters and available to all the entities. |
| **DRAWBACKS:-**   * It fails to achieve privacy, data dynamics. * It fails to support batch auditing property. * It reduces storage and maintenance cost of the data owner. | **ADVANTAGES:-**   * to support data dynamics. * Auditor can be able to verify the integrity of all the desired blocks at once by checking a block. * Any third party other than DU should be able to correctly verify the integrity of the data stored in CSP. |

**System model with a cloud server, a data owner and**

**data users.**

****

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE