SEPDP Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage

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.

**EXISTING SYSTEM**

* Remote data integrity checking protocols can be broadly categorized into two kinds. The deterministic guarantee based schemes like [17] [18] and [19], verify each block of data and therefore require a significant amount of storage and computation. Alternative kind of schemes called provable data possession (PDP) includes [8], [3], [20] use probabilistic checking method, in which a few blocks are randomly selected to detect manipulation. PDP is introduced in [8] that use random sampling of a few blocks for integrity verification.
* Shacham et al. [3] designed two different integrity verification mechanisms. One uses pseudo-random function (PRF) which fails to provide public verifiability, while the other one uses boneh–lynn–shacham (BLS) signatures [20]. Both the schemes support blockless verification but fail to provide privacy of the DO’s data. Blockless verification requires linear combination of sampled blocks which gives a clue to TPA to extract the data [4].
* To preserve privacy of the data owner supporting blockless verification, Wang et al. [4] proposed a public auditing scheme and extended that to support batch auditing further. As a result, TPA can simultaneously perform multiple auditing requests from different DUs. But, all these schemes [3], [4], [8] fail to support data dynamics. Moreover, as signatures of the data blocks contain index number of the corresponding blocks, if one block is updated (inserted/modified/deleted), the corresponding verification meta-data (signature) of all other blocks need to be updated. The scheme proposed in [16] uses index hash table (IHT) to support data dynamics in public auditing mechanism reducing the update overhead.
* Unfortunately, this scheme fails to support batch auditing property. later on, Wang et al. [7] extended their previous technique [4] to support data dynamics. Yang et al. [11] proposed an efficient and secure dynamic auditing protocol that achieves all essential features of public auditing. Also it consumes lesser computation and communication cost. A certificateless public auditing scheme for verifying data integrity in the cloud is proposed by Wang et al. [2].
* Although this scheme does not require certificate for key generation, it fails to achieve privacy, data dynamics, and batch auditing properties. But, [2], [3], [4], [8], [11], [15], [16] schemes are based on pairing based cryptography, which requires more verification cost in audit phase.
* **Disadvantages**
* There is less security on outsourced data due to lack of Verification Based on Hash code.
* There is no more security in the data access.

**PROPOSED SYSTEM**

* In the proposed work, the system proposes a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPDP is that it does not use any intensive computation like pairing based operation.
* Further, the system extends SEPDP 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 SEPDP is efficient and suitable to implement the verification at the low powered devices.

**Advantages**

* The Data Security is more due to Data integrity Proof.
* The strong 256 bit security Key and Hash code are implemented.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL