A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage

ABSTRACT:

As an important application in cloud computing, cloud storage offers user scalable, flexible and high quality data storage and computation services. A growing number of data owners choose to outsource data files to the cloud. Because cloud storage servers are not fully trustworthy, data owners need dependable means to check the possession for their files outsourced to remote cloud servers. To address this crucial problem, some remote data possession checking (RDPC) protocols have been presented. But many existing schemes have vulnerabilities in efficiency or data dynamics. In this paper, we provide a new efficient RDPC protocol based on homomorphic hash function. The new scheme is provably secure against forgery attack, replace attack and replay attack based on a typical security model. To support data dynamics, an operation record table (ORT) is introduced to track operations on file blocks. We further give a new optimized implementation for the ORT which makes the cost of accessing ORT nearly constant. Moreover, we make the comprehensive performance analysis which shows that our scheme has advantages in computation and communication costs. Prototype implementation and experiments exhibit that the scheme is feasible for real applications.

EXISTING SYSTEM:

- The first RDPC was proposed by Deswarte et al. based on RSA hash function. The drawback of this scheme is that it needs to access the entire file blocks for each challenge.
In 2007, the provable data possession (PDP) model was presented by Ateniese et al., which used the probabilistic proof technique for remote data integrity checking without accessing the whole file. In addition, they supplied two concrete schemes (S-PDP, E-PDP) based on RSA.

Although these two protocols operations had good performance, it's a pity they didn't support dynamic operations. To overcome this shortcoming, in 2008, they presented a dynamic PDP scheme by using symmetric encryption. Nonetheless, this scheme still did not support block insert operation. At the same time, lots of research works devoted to construct fully dynamic PDP protocols. For instance, Sebé et al. provided a RDPC protocol for critical information infrastructures based on the problem to factor large integers, which is easily adapted to support data dynamics.

**DISADVANTAGES OF EXISTING SYSTEM:**

- Did not Support Dynamic Operations.
- Heavy Computation Cost.
- Insecure against replay attack and deletion attack.
- These schemes are either insecure or not efficient enough.

**PROPOSED SYSTEM:**

We present a novel efficient RDPC scheme with data dynamics. The basic scheme utilizes homomorphic hash function technique, in which the hash value of the sum for two blocks is equal to the product for two hash values of the corresponding blocks.
We introduce a linear table called ORT to record data operations for supporting data dynamics such as block modification, block insertion and block deletion. To improve the efficiency for accessing ORT, we make use of doubly linked list and array to present an optimized implementation of ORT which reduces the cost to nearly constant level.

We prove the presented scheme is secure against forgery attack, replay attack and replace attack based on a typical security model. At last we implement our scheme and make thorough comparison with previous schemes.

ADVANTAGES OF PROPOSED SYSTEM:

- Experiment results show that the new scheme has better performance and is practical for real applications.
- We show the advanced RDPC scheme supporting fully dynamic block operations based on ORT.
- Minimum Computation Costs.
- The data owner can perform dynamic operations of the files

SYSTEM ARCHITECTURE:

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:
System : Pentium Dual Core.
Hard Disk : 120 GB.
Monitor : 15” LED
Input Devices : Keyboard, Mouse
Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Hao Yan, Jiguo Li, Jinguang Han, Member, IEEE and Yichen Zhang, “A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage”, IEEE 2017