A Novel Efficient Remote Data PossessionChecking Protocol in Cloud Storage

ABSTRACT:

As an important application in cloud computing,cloud storage offers user scalable, flexible and high quality datastorage and computation services. A growing number of dataowners choose to outsource data files to the cloud. Because cloudstorage servers are not fully trustworthy, data owners needdependable means to check the possession for their filesoutsourced to remote cloud servers. To address this crucialproblem, some remote data possession checking (RDPC) protocolshave been presented. But many existing schemes havevulnerabilities in efficiency or data dynamics. In this paper, weprovide a new efficient RDPC protocol based on homomorphichash function. The new scheme is provably secure against forgeryattack, replace attack and replay attack based on a typicalsecurity model. To support data dynamics, an operation recordtable (ORT) is introduced to track operations on file blocks. Wefurther give a new optimized implementation for the ORT whichmakes the cost of accessing ORT nearly constant. Moreover, wemake the comprehensive performance analysis which shows thatour scheme has advantages in computation and communicationcosts. Prototype implementation and experiments exhibit that thescheme 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 itneeds to access the entire file blocks for each challenge.

- In 2007,the provable data possession (PDP) model was presented byAteniese et al., which used the probabilistic prooftechnique for remote data integrity checking without accessingthe 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 dynamicoperations.To overcome this shortcoming, in 2008, theypresented a dynamic PDP scheme by using symmetricencryption. Nonetheless, this scheme still did not supportblock insert operation. At the same time, lots of research worksdevoted to construct fully dynamic PDP protocols. Forinstance, Sebé et al. provided a RDPC protocol for criticalinformation infrastructures based on the problem to factor largeintegers, 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:

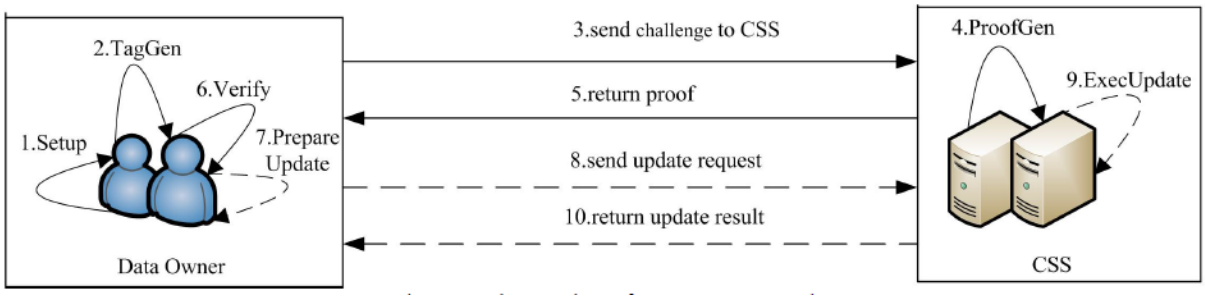
- We present a novel efficient RDPC scheme with data dynamics. The basic scheme utilizes homomorphic hashfunction technique, in which the hash value of the sum for twoblocks is equal to the product for two hash values of thecorresponding blocks.

- We introduce a linear table called ORTto record data operations for supporting data dynamics such asblock modification, block insertion and block deletion. Toimprove the efficiency for accessing ORT, we make use ofdoubly linked list and array to present an optimizedimplementation of ORT which reduces the cost to nearlyconstant level.
- We prove the presented scheme is secure againstforgery attack, replay attack and replace attack based on atypical security model. At last we implement our scheme andmake 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:

- Operating system : Windows 7.
- 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 PossessionChecking Protocol in Cloud Storage", IEEE 2017