Identity-based Remote Data Integrity Checking withPerfect Data Privacy Preserving for Cloud Storage

ABSTRACT:

Remote data integrity checking (RDIC) enables adata storage server, say a cloud server, to prove to a verifier thatit is actually storing a data owner's data honestly. To date, anumber of RDIC protocols have been proposed in the literature,but most of the constructions suffer from the issue of a complexkey management, that is, they rely on the expensive public keyinfrastructure (PKI), which might hinder the deployment ofRDIC in practice. In this paper, we propose a new constructionof identity-based (ID-based) RDIC protocol by making use ofkey-homomorphic cryptographic primitive to reduce the systemcomplexity and the cost for establishing and managing the publickey authentication framework in PKI based RDIC schemes.We formalize ID-based RDIC and its security model includingsecurity against a malicious cloud server and zero knowledgeprivacy against a third party verifier. The proposed ID-basedRDIC protocol leaks no information of the stored data to theverifier during the RDIC process. The new construction is provensecure against the malicious server in the generic group modeland achieves zero knowledge privacy against a verifier. Extensivesecurity analysis and implementation results demonstrate thatthe proposed protocol is provably secure and practical in thereal-world applications.

EXISTING SYSTEM:

- Wang et al. proposed the notion of "zeroknowledgepublic auditing" to resist off-line guessing attack.

- Yu et al. recently enhanced the privacy of remote data integrity checking protocols for secure cloud storage, but theirmodel works only in public key infrastructure (PKI) basedscenario instead of the identity-based framework.
- Wang proposed another identity-based provable data possession in multi-cloud storage.

DISADVANTAGES OF EXISTING SYSTEM:

- MHT itself is not enough to verify the block indices, which may lead to replace attack.
- A formal security model is not provided.
- But theirmodel works only in public key infrastructure (PKI) basedscenario instead of the identity-based framework

PROPOSED SYSTEM:

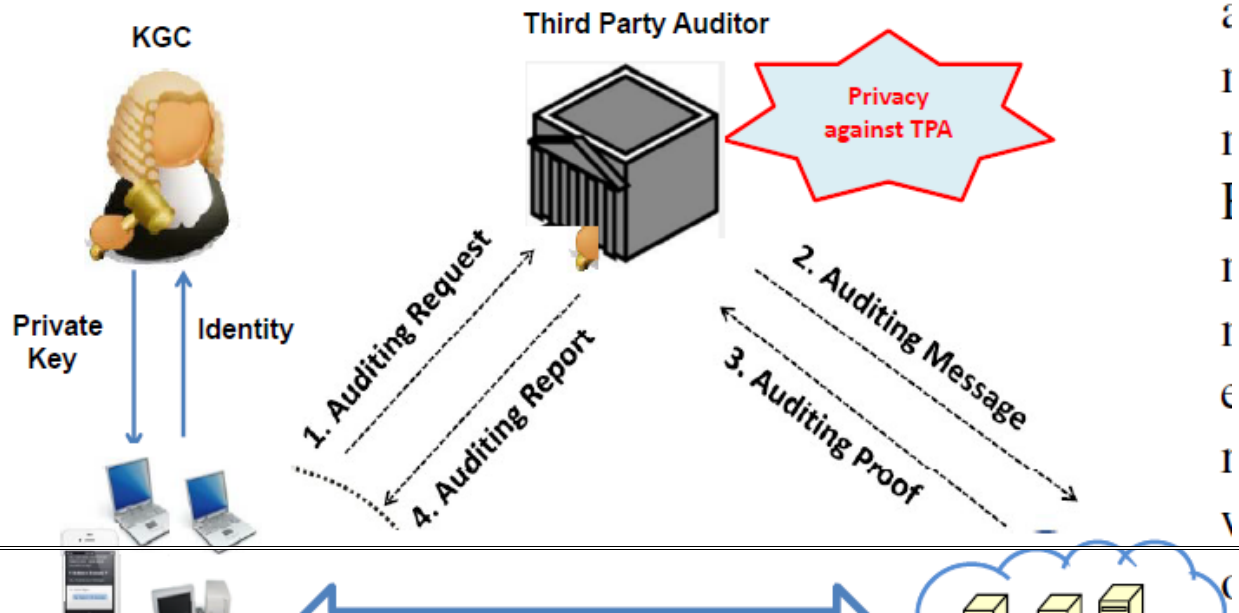
- In an ID-based signature scheme, anyone with accessto the signer's identity can verify a signature of thesigner. Similarly, in ID-based RDIC protocols, anyoneknowing a cloud user's identity, say a third party auditor(TPA), is able to check the data integrity on behalf of thecloud user. Thus, public verifiability is more desirablethan private verification in ID-based RDIC, especiallyfor the resource constrained cloud users. In this case, theproperty of zero-knowledge privacy is highly essential fordata confidentiality in ID-based RDIC protocols.
- Our firstcontribution is to formalize the security model of zeroknowledgeprivacy against the TPA in ID-based RDICprotocols for the first time.

- We fill the gap that there is no a secure and novel IDbasedRDIC scheme to date. Specifically, we proposea concrete ID-based RDIC protocol, which is a novelconstruction that is different from the previous ones,by making use of the idea of a new primitive calledasymmetric group key agreement.
- To be morespecific, our challenge-response protocol is a two partykey agreement between the TPA and the cloud server, thechallenged blocks must be used when generating a sharedkey, which is a response to a challenge from the TPA, bythe cloud server.
- We provide detailed security proofs of the new protocol,including the soundness and zero-knowledge privacy ofthe stored data. Our security proofs are carried out in thegeneric group model.

ADVANTAGES OF PROPOSED SYSTEM:

- This is the first correct security proof of ID-based RDIC protocol. Thus, the new security proof method itself may be of independent interest.
- We show the practicality of the proposal by developing a prototype implementation of the protocol.

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:

Yong Yu, Man Ho Au_, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-based Remote Data Integrity Checking withPerfect Data Privacy Preserving for Cloud Storage", **IEEE Transactions on Information Forensics and Security, 2017.**