Volume No:2, Issue No:6 (November-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Unique Identity-Based Uploading and Remote Data Integrity Checking In Public Cloud

M.Damodhar, M.Tech
Academic Consultant,
S. V. U. C. E,
S. V. University.

A.Nagarjuna, M.Tech
Academic Consultant,
S. V. U. C. E,
S. V. University.

Abstract:
Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (Identity-Based Distributed Provable Data Possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of Elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

Index Terms:
Cloud storage, Remote data integrity, Multi-cloud servers, Identity-based distributed provable data possession (ID-DPDP).

INTRODUCTION:

Advances in networking and computing technologies have prompted many organizations to outsource their storage needs on demand. This new economic and computing paradigm is commonly referred to as cloud storage. It brings appealing benefits including relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, Software, and personnel maintenances, etc. However, there are barriers that hinder migration to the cloud. One of the main barriers is that, due to lack of physical control over the outsourced data, a cloud user may worry about whether her data are kept as expected. If the cloud user is a company, apart from the risk of remote malicious attacks on the cloud, the traditional concerns posed by malicious company insiders are now supplemented by the even more hazardous threat of malicious outsiders who are given the power of insiders. A recent EU bill forces companies migrating to the cloud to be liable for any data corruption or privacy breach into which their cloud service provider (CSP) may incur, even when they do not retain control over their data. Convincing cloud users that their data are intact is especially vital when users are companies. Remote data possession checking (RDPC) is a primitive designed to address this issue.

A. Remote Data Possession Checking:

RDPC allows a client that has stored data at a public cloud server (PCS) to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication.

Volume No:2, Issue No:6 (November-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In order to achieve secure RDPC implementations, Ateniese et al. proposed a provable data possession (PDP) paradigm and designed two provably-secure PDP3 schemes based on the difficulty of large integer factoring. They refined the original paradigm and proposed a dynamic PDP scheme in but their proposal does not support the insert operation. In order to solve this problem, Erway et al. proposed a full-dynamic PDP scheme by employing an authenticated flip table. Following Ateniese et al.'s pioneering work, researchers devoted great efforts to RDPC with extended models and new protocols. One of the variations is the proof of retrievability (POR), in which a data storage server cannot only prove to a verifier that he is actually storing all of a client's data, but also it can prove that the users can retrieve them at any time.

This is stronger than the regular PDP notion. Shacham presented the first POR schemes with provable security. The state of the art can be found in but few POR protocols are more efficient than their PDP counterparts. The challenge is to build POR systems that are both efficient and provably secure. Note that one of benefits of cloud storage is to enable universal data access with independent geographical locations. This implies that the end devices may be mobile and limited in computation and storage. Regular RDPC protocols are more suitable for cloud users equipped with mobile end devices. Our ID-RDPC architecture and protocol are based on the PDP model.

B. Motivation and Contribution:

This approach focuses on RDPC in company-oriented cloud storage. Consider a scenario in which a company purchases the cloud storage service. Only the staff members of the company are allowed to upload data to the PCS and may check the integrity of their data with mobile devices. PCS has to be convinced that the data (and their tags) to be uploaded come from the staff of the company, although this step is usually omitted in the existing models. The metadata or the tags are indeed signatures of the original data.

Note that the existing RDPC protocols are designed in the PKI setting. PCS needs to validate the tags and the appended public key certificate of the users. The validation of the legit uploads incurs considerable overheads since the staff may 4 frequently upload data to PCS. This burden can only be partially mitigated by letting PCS cache the verified certificates. Indeed, caching cannot be used for certificates revoked before their expiration, for employees who leave the company, for newly recruited employees, etc. In addition to the heavy certificate verification, the system suffers from complicated certificate management: certificates generation, delivery, revocation, renewal, etc. In order to solve the above problem, we investigate a new RDPC model incorporating identity based cryptography, i.e., the ID-RDPC model. Our contribution is twofold:

- First, we formalize the ID-RDPC model. In this model, a trusted private key generator (PKG) generates the system public key and the master secret key. The PKG also generates private keys for the clients, i.e., the staff members of the company, by taking as input the staff members' identities and the PKG's master secret key. With a private key, the client can generate the tags of the data to be uploaded. Upon receiving a request of a data possession proof, the PCS can generate the proof without verifying any certificate but simply checking that the corresponding system public key is from a company allowed to use the service. Finally, the client can verify whether the PCS-generated proof is valid.
- Second, we realize the first ID-RDPC protocol. The main challenge to design the ID-RDPC protocol is that it requires the client to generate aggregately ID-based signatures like tags without applying the hash-and-sign paradigm to the original data. We address this with a variation of the well-known Schnorr signature. The instantiated ID-RDPC protocol is shown to be secure by assuming the hardness of the Computational Diffie-Hellman problem. In addition to the structural advantage of

Volume No:2, Issue No:6 (November-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

eliminating certificate management and verification, our ID-RDPC protocol is more efficient than the existing RDPC protocols in the PKI setting in terms of computation and communication.

EXISTING SYSTEM:

In public cloud environment, most clients upload their data to Public Cloud Server (PCS) and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the period of investigation. When a large of data is generated, who can help him process these data? If these data cannot be processed just in time, the manager will face the loss of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary.

But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager's remote data integrity unless he is delegated by the manager. We call the secretary as the proxy of the manager. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity.

Disadvantages of Existing System:

- In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, etc.
- In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, etc.

PROPOSED SYSTEM:

In public cloud, this paper focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. We give the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, we designed the first concrete ID-PUIC protocol. In the random oracle model, our designed ID-PUIC protocol is provably secure. Based on the original client's authorization, our protocol can realize private checking, delegated checking and public checking.

Advantages of Proposed System:

- The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis

SYSTEM ARCHITECTURE:

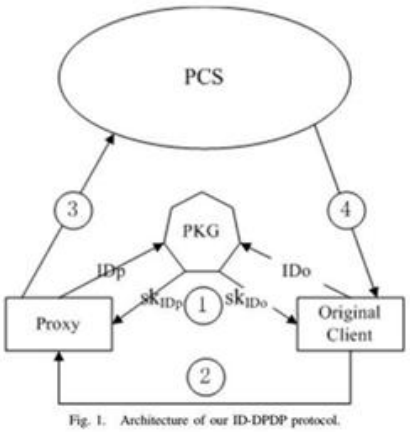

Fig. 1. Architecture of our ID-DPDP protocol.

Volume No:2, Issue No:6 (November-2016) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

MODULES:

1. Original Client Module
2. Public Cloud Server Module
3. Proxy Module
4. Key Generation Center (KGC) Module

Module Description:

Original Client:

An entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

PCS (Public Cloud Server):

An entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.

Proxy:

An entity, which is authorized to process the Original Client's data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant mω which is signed and issued by Original Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

KGC (Key Generation Center):

An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

CONCLUSION:

Favorable solutions to ensure data privacy must employ flexible data perturbation methods that provide control over the tradeoff between the privacy guarantee and the utility of the query results. Prevent dynamic data integrity among applications hosted by different cloud systems. Proxy services are implemented to maintain the authentication and initially provide support for simple use cases, later progressing to more complex use cases.

REFERENCES:

1. Huaqun Wang, Debiao He, and Shaohua Tang "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud" IEEE TRANSACTIONS ONINFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016.

2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song. Provable Data Possession at Untrusted Stores.CCS'07, pp. 598-609, 2007.

3. G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik. Scalable and Efficient Provable Data Possession. Secure Comm. 2008, article 9, 2008.

4. C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia. Dynamic Provable Data Possession.CCS'09, 213-222, 2009.

5. F. Seb´e, J. Domingo-Ferrer, A. Martınez-Ballest´e, Y. Deswarte, J. Quisquater. Efficient Remote Data Integrity checking in Critical Information Infrastructures. IEEE Transactions on Knowledge and Data Engineering, 20(8):1034-1038, 2008.

6. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau. Efficient Provable Data Possession for Hybrid Clouds. CCS'10, 756-758, 2010.

7. Y. Zhu, H. Hu, G.J. Ahn, M. Yu. Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, 23(12):2231-224, 2012.

8. R. Curtmola, O. Khan, R. Burns, G. Ateniese. MR-PDP: Multiple Replica Provable Data Possession. ICDCS'08, 411-420, 2008.