Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage

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.
EXISTING SYSTEM:

In cloud computing, remote data integrity checking is an important security problem. The clients’ massive data is outside his control. The malicious cloud server may corrupt the clients’ data in order to gain more benefits. The formal system model and security model are existing models.

In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a probabilistic proof of possession by sampling random set of blocks from the server, which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model.

In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. It results in the third party auditing in cloud computing.
PROBLEM DEFINITION:

- Does not provide efficiency in remote data integrity checking.
- More expensive.
- The existing system provides less flexibility.

PROPOSED SYSTEM:

Remote data integrity checking is of crucial importance in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. We propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffi Hellman) problem. The proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

ADVANTAGES OF PROPOSED SYSTEM:

- The distributed cloud storage is indispensable.
- Efficient and Flexible.
- Elimination of the certificate management.
SYSTEM ARCHITECTURE:

![System Architecture Diagram]

HARDWARE REQUIREMENTS:

- **System**: Pentium IV 2.4 GHz.
- **Hard Disk**: 40 GB.
- **Floppy Drive**: 1.44 Mb.
- **Monitor**: 15 VGA Colour.
- **Mouse**: Logitech.
- **Ram**: 512 Mb.

SOFTWARE REQUIREMENTS:
IEEE Projects 100% WORKING CODE + DOCUMENTATION+ EXPLANATION – BEST PRICE
LOW PRICE GUARANTEED

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net
- Tool : Visual Studio 2010
- Database : SQL SERVER 2008