Towards Secure Data Distribution Systems in Mobile Cloud Computing

ABSTRACT

Cloud computing, many computing resources are provided as services over the internet. One of the main services provided by clouds is storage (e.g., Simple Storage Services—Amazon S3), which allows users to store their enormous amount of data to the remote clouds without bothering the complex management of storage hardware. Outsourcing big data to clouds provides many benefits, e.g., low costs, good reliability and availability, but the data security issues such as privacy and integrity brought by third party's cloud systems have been the major concerns for users utilizing such services. Since the data is stored and managed in the cloud, the data security highly depends on the IT management of the cloud services providers, and any security loophole in the cloud system might damage the security of the users' private data.

EXISTING SYSTEM

In Existing System, we present an efficient data distribution system in MCC, which allows mobile users to securely store their data in the cloud storage, and flexibly share their data with friends. We leverage several cryptographic primitives to achieve data privacy, data integrity, dynamical data modification and deletion, and flexible data distribution. Concretely, we first design an efficient type-based proxy re-encryption (TB-PRE), which allows a mobile user with a single secret key to keep the data privacy, and flexibly share his data with friends under permission. We also use the BLS signature to both protect the integrity of the data and provide authentication to the data.

DIS ADVANTAGES

- Damage the security of the users' private data.
- It does not support dynamic data distribution.

PROPOSED SYSTEM

In Proposed System, we leverage several cryptographic primitives such as a new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC,

which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, our system is a lightweight and easily deployable solution for mobile users in MCC since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations. Finally, we present extensive performance analysis and empirical studies to demonstrate the security, scalability, and efficiency of our proposed system.

ADVANTAGES

- Data with strong privacy and security protection.
- It achieves data integrity, dynamical data modification and deletion, and flexible data distribution.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp

Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC