Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage

ABSTRACT:

The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.

INTRODUCTION

TO DATE many individuals and companies choose to upload their data to clouds since the clouds supports considerable data storage service but also efficient data processing capability. Accordingly, it is unavoidable that trillions of personal and industrial data are flooding the Internet. For example, in some smart grid scenario, a governmental surveillance authority may choose to supervise the electricity consumption of a local living district. A great amount of electricity consumed data of each family located inside the district will be automatically transferred to the authority via Internet period by period. The need of big data storage, therefore, is more desirable than ever.

EXISTING SYSTEM

In Existing System a basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing
cryptographic encryption mechanisms can be employed to fulfill the requirement. For instance, Public Key Encryption (PKE) allows a data sender to encrypts the data under the public key of receiver such that no one except the valid recipient can gain access to the data.

DisADVANTAGE OF Existing SYSTEM

- Does not satisfy all the requirements of users in the scenario of big data storage.
- Job execution time.

PROPOSED SYSTEM

In Proposed System a concrete construction for unidirectional AMH-IBCPRE, in which it achieves multiple ciphertext receiver update, conditional data sharing, anonymity and collusion-safe (i.e. holding against collusion attacks) simultaneously in asymmetric bilinear group. Note the functionality of our system is generally described in Fig 1. We state that the new primitive is applicable to many real-world applications, such as secure email forwarding, electronic encrypted data sharing, where both anonymity and flexible encrypted data sharing are needed. We also show that the scheme is CCA-secure in the standard model under the decisional P-Bilinear Diffie-Hellman assumption. To the best of our knowledge, our system is the first of its kind in the literature.

ADVANTAGE OF PROPOSED SYSTEM

- Anonymity: given a ciphertext, no one knows the identity information of sender and receiver.
- Multiple receiver-update: given a ciphertext, the receiver of the ciphertext can be updated in multiple times.
- Conditional sharing: a ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied.
ARCHITECTURE:
HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 44 Mb.
- Monitor: 15 VGA Colour.

SOFTWARE REQUIREMENTS:

- Coding Language: Java 1.7, Hadoop 0.8.1
- Database: MySql 5
- IDE: Eclipse