CIRCUIT CIPHERTEXT POLICY ATTRIBUTE BASED HYBRID ENCRYPTION WITH VERIFIABLE DELEGATION IN CLOUD

ABSTRACT

In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work.

EXISTING SYSTEM

The cloud servers can offer various data services, such as remote data storage and outsourced delegation computation. Since the cloud server may not be credible, the file cryptographic storage is an effective method to prevent private data from being stolen or tampered. In the meantime, they may need to share data with the person who satisfies some requirements. The work of delegation is promising but inevitably suffers from two problems. a) The cloud server might replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext. b)The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible.

DISADVANTAGES

- Data stored in cloud server is to be stolen or tampered.
- Cloud server cheat the authorized user for cost saving

PROPOSED SYSTEM

In this paper we proposed the generic key encapsulation mechanism (KEM)/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption.Such improved model has the advantage of achieving higher security requirements. ABE with verifiable delegation.Since the introduction of ABE, there have been advances in multiple directions. the first ABE with outsourced decryption scheme to reduce the computation cost during decryption.

ADVANTAGES:

- the data is confidentiality.
- It provides a fine grained access control.
- The data is security against attack.
- The solution is feasibility and efficiency.

SYSTEM REQUIREMENTS:

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:

Operating system : - Windows XP.

Coding Language : JAVA

Data Base : SQL Server 2005.