A collaborative key Management protocol in cipher text policy attribute Based Encryption for Cloud Data sharing

Abstract:

we propose a novel collaborative key management protocol to increase both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system. Distributed key generation, issue and storage of private keys are realized without adding any extra physical infrastructure. We introduce attribute groups to build a private key update algorithm for fine-grained and immediate attribute revocation.

Existing system:

The key authority must be completely trustworthy, as it can decrypt all the cipher text using a Generated private key without permission of its owner. This is commonly called the key escrow problem and is one disadvantage. mobile front-end devices, such as smart phones, are far more vulnerable than servers with respect to privacy protection Thus, the vulnerability in private key protection may easily lead to the exposure of keys to unauthorized users .In addition, current ABE key management schemes also require much bilinear pairing calculation, exponentiation and multiplication, especially in the decryption The resulting run time may be horribly unacceptable.

Disadvantages:

1. Security problems and key exposure chances are there.
2. The time required for decryption takes large value.

Proposed system:

We propose a novel collaborative key management protocol in cipher text policy attribute-based Encryption (CKM-CP-ABE) aiming to enhance security and efficiency of key management in cloud data sharing system.

Further Details Contact: A Vinay 9030333433, 08772261612, 9014123891
#301, 303 & 304, 3rd Floor, AVR Buildings, Opp to SV Music College, Balaji Colony, Tirupati - 515702
Email: info@takeoffprojects.com | www.takeoffprojects.com

1) A novel collaborative protocol is presented. With help of that secure key management is guaranteed which is more easy to deploy compared with previous multi-authority schemes.
2) A unique attribute group key is allocated to each attribute group that contains clients who share the same attribute. Via updating attribute group key, a fine-grained and immediate attribute revocation is provided.
3) The collaborative mechanism helps markedly reduce client decryption overhead by employing a decryption server to execute most of decryption while leave no knowledge about information to it.

Advantages:

1. Secure key management and unique group key generation provided so that security problems will not be there.

2. For reducing the decryption time overhead we have proposed special methods here

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