**Secure Data Sharing in A Proxy Re-Encryption Data**

**ABSTRACT: -**

Proxy re-encryption (PRE) provides a promising solution for encrypted data sharing in public cloud. When data owner Alice is going to share her encrypted data with data consumer Bob, Alice generates a re-encryption key and sends it to the cloud server (proxy); by using it, the proxy can transform Alice’s ciphertexts into Bob’s without learning anything about the underlying plaintexts. Despite that existing PRE schemes can prevent the proxy from recovering Alice’s secret key by collusion attacks with Bob, due to the inherent functionality of PRE, it is inevitable that the proxy and Bob together are capable to gain and distribute Alices decryption capabilities. Even worse, the malicious proxy can deny that it has leaked the decryption capabilities and has very little risk of getting caught.To tackle this problem, we introduce the concept of Accountable Proxy Re-Encryption (APRE), whereby if the proxy is accused to abuse the re-encryption key for distributing Alice’s decryption capability, a judge algorithm can decide whether it is innocent or not. We then present a non-interactive APRE scheme and prove its CPA security and accountability under DBDH assumption in the standard model. Finally, we show how to extend it to a CCA secure one

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * Even worse, the malicious proxy can deny that it has leaked the decryption capabilities and has very little risk of getting caught. * This weakness is also called re-encryptionkey abuse problem. * The Security against maliciousdelegator | * We provethat our scheme is CPA secure, secure against malicious. * proxy and secure against malicious delegator under the DBDHassumption in the standard model. * Furthermore, we extend itto a CCA secure one by employing a generic transformation |
| **EXISTING ALGORITHM**  CCASecure One | **PROPOSED ALGORITHM: -**  Proxy Re-Encryption(PRE) |
| **ALGORITHM DEFINITION: -**  Forany PRE scheme s, we instantiate the experiment with aCPA adversary A and = 2. It is required that pk isuncorrupted and jm0j = jm1j. | **ALGORITHM DEFINITION: -**  The traditional security notion of PRE focuses on preventingthe proxy from learning anything about the encrypted messages.However, it is not enough to realize the applicationrequirement shown in the above example. Due to the inherentfunctionality of PRE, the cloud server and Bob together areable to obtain Alice’s decryption capability and keep it on anyform of carriers, such as a decryption program or a decryptiondevice1. Therefore, Alice’s decryption capability could besold online and offline, which makes Alice suffering seriouseconomic losses. This weakness is also called re-encryption  key abuse problem. |
| **DRAWBACKS: -**   * Less Security * Prone to keyword guessing attacks | **ADVANTAGES: -**   * High Security * Multiple levels of access and security |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE