N.Veeraragavan *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 94-100 **ISSN: 2321-8363**

PROXY RE-ENCRYPTION USING HYBRID ENCRYPTION SCHEME SECURE AGAINST CHOSEN CIPHERTEXT ATTACK

N.Veeraragavan[1], Mr.S.Rajesh[2]

[1]PG Student, [2]Assistant Professor, Department of Computer Science and Engineering,

PRIST University, Trichy District, India

([1] Veeraraghavan543@gmail.com)

Abstract

The objective is to present the unidirectional proxy re-encryption scheme with chosen-cipher text security. The goal of Proxy Re-Encryption system is to securely enable the re-encryption of cipher texts from one key to another, without relying on trusted parties. A Proxy can transform - without seeing the Plaintext - cipher text encrypted under one key into an encryption of the same plaintext under another key. Proxy Re-Encryption is a form of public-key encryption that allows a user Alice to "delegate" her decryption rights to another user Bob. In a PRE scheme, a proxy is given a piece of information that allows turning a cipher text encrypted under a given public key into an encryption of the same message under a different key.

Full Text: www.ijcsma.com/publications/january2014/V2I113.pdf