Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.10 – 14

RESEARCH ARTICLE

Secure Transaction System Using ID Based Cryptography

Jaydipsinh B. Jadeja[*], Harikrishna Jethva[**], Bhadreshsinh G. Gohil [***]

*(PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University, Ahmedabad
Email: jaydip189@gmail.com)
** (Associate Professor, L D Engineering College, Ahmedabad
Email: hbjethva@gmail.com)
*** (Assistant Professor, SIEM, Rajpur, Mehsana
E-mail: bhadu.gohil@gmail.com)

Abstract— Today more and more number of clients are using online transactions, and so online transaction systems are becoming more desirable targets for security attacks. To maintain the clients trust and confidence in the security of their online transaction application, financial firm must identify how attackers compromise accounts and develop methods to protect them. Towards this purpose, we present a modified model to authenticate clients for online transaction transactions through utilizing Identity-Based Cryptography techniques in conjunction with the one-time ID concept for the purpose of increasing security. Identity-based public key encryption facilitates easy introduction of public key cryptography which allows an entity's public key to be derived from an arbitrary id value, such as name or email address or birthdate. The main practical benefit of identity-based cryptography is in greatly reducing the need for, and reliance on, public key certificates. Although some interesting identity-based techniques have been developed in the past, none are compatible with popular public key encryption algorithms. This limits the utility of identity-based cryptography as a transitional step to full-blown public key cryptography. Furthermore, it is fundamentally difficult to reconcile fine-grained revocation with identity-based cryptography. Using ID based cryptography we can enhance the performance of transaction management system with high level security. A noble approach will be selected to provide a solution for secure key exchange for transaction purpose with enhanced security.

Keywords— ID Based Cryptography; Mediated rsa; Transaction System

Full Text: http://www.ijcsmc.com/docs/papers/December2013/V2I12201303.pdf