© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Enchancement of security of firewall based cloud server using customized DES

[1]Poonam Verma, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor , Department of CSA, CDLU Sirsa

ABSTRACT: In this dissertation a PicPass algorithm is proposed for the solution of Key Exchange problem using Symmetric and Asymmetric key cryptography. Diffie and Hellman proposed an algorithm for key exchange. But this algorithm suffers from Man-in middle attack. So to overcome this problem Seo proposed another algorithm that uses text password for the agreement between two parties. But again the password suffers from offline dictionary attack. In this, a PicPass Protocol i.e. picture is used as a password to make an agreement between two parties. The protocol contains two function i.e. picture function as well as distortion function is used to make picture in a compact size and then it is sent to receiver. Firstly the sender encrypts the Plain Text using Secret Picture and creates the Cipher Text using Symmetric key cryptography. Then the Secret Picture will be encrypted by covered picture resulting into Encrypted Picture. Now the Cipher Text and Encrypted Picture will be placed into digital envolpe and then the envelope will be send to the receiver. The receiver will receive the digital envelope, open it and then decrypt the Encrypted Picture using his Key Picture.

[1] Introduction

Basics of Cryptography

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

2 Cryptosystem

Encryption is a method of transforming original data, called **plaintext** or **cleartext**, intoa form that appears to be random and unreadable, which is called **ciphertext**. Plaintextis either in a form that can be understood by a person (a document) or by a computer(executable code). Once it is transformed into ciphertext, neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without unauthorized disclosure. When data isstored on a computer, it is usually protected by logical and physical access controls.When this same sensitive information is sent over a network, it can no longer take thesecontrols for granted, and the information is in a much more vulnerable state.