International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 143-148

SECURE IMAGE SHARING WITH ENCRYPTION OF BLOWFISH, AES AND RC4 HYBRID ALGORITHM WITH HASH FUNCTION

RAVINDER KAUR[1], PANKAJ SHARMA[2] & MEENAKSHI SHARMA[3]

[1]M.Tech Student, Department of CSE, Sri Sai College of Engg. and Technology, Pathankot, Badhani, Punjab, India

[2]Assistant Professor, Department of CSE, Sri Sai College of Engg. and Technology, Pathankot, Badhani, Punjab, India

[3]Associate Professor, Department of CSE, Sri Sai College of Engg. and Technology, Pathankot, Badhani, Punjab, India

ABSTRACT

Grid computing is a distributed network in which several processors distributed globally and sharing the computational resources to solve various problems. Security in every network is now a must and important part for the successful communication in network. Normally network security is at much higher level on outer part of the network than the inside part. This property of security sometime can act as hot cake for network intruders. Insider attacks combined with various worm attacks could prove to be the bottleneck and disaster for network. There is need of optimized approaches to handle such security issues. In our research we will focus on the combination of Advance Encryption Standard (AES) and Rivest Cipher version 4 (RC4) to provide strong combination of encryption to defend against discussed security concerns and then provide some hiding functions with help of hash functions such as MD5 or SHA1. Advance encryption standard (AES) provides solution for security with whitener (Whitening is used to enhance the security of the cipher) with multiple matrix in RC4 algorithm which is ten converted with hash function for best secure communication. Combination will prove to be best fit for providing security with secret key to each and every block of AES combined with whitened text. RC4 will produce multiple three layer matrix with different combination to enhance security which is finally interated with hash function for providing hashed data which will provide more security in communication. Blowfish is a symmetric blockcipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securingdata. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses.

KEYWORDS: Advance Encryption Standard, Rivest Cipher, Message Digest Level 5, SHA1, Grid Computing, Whiten Text, Bluefish