International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.
It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 4, Issue 9, September 2016.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

A STUDY ON IMPROVING THE SECURITY AND PERFORMANCE OF AES ALGORITHM FROM SIDE CHANNEL ATTACKS USING CLOUD

M. NAVANEETHA KRISHNAN [1] , DR.R.RAVI [2]
[1]Research Scholar, Department of Computer Science and Engg, Manonmaniam Sundarnar University, Thirunelveli, India
mnksjce@gmail.com

[2]Professor & HOD, Department of Information Technology, Francis Xavier Engg College, Thirunelveli, India
directorresearch@francisxavier.ac.in

Abstract — Cloud services which are fast developing has its own vulnerabilities in the recent past. This paper attempts to set up a secret cloud atmosphere, making obvious a cache based side channel attack and travel around solutions to counter offense the same. A Cloud Computing location to host the attack and preventing the same is set up using an release source software called OpenStack. Based on side channel in sequence obtained from the encryption device in addition to the attack by any brute force is termed as side channel attack. The various types of side channel attacks are, acoustic cryptanalysis attack, timing attack, differential fault analysis, power monitoring attack, data remanence attack and row humor attack. Timing attack make use of timing in revolve and extra input that are made available throughout the usual performance in encryption device. Power monitoring attack measures the control utilization of the cryptographic machine and check the association between instant power spending and secret key information. Repossession of erased data that are available even after more than a few effort are made to take away those is called Data remanence. It creates instinctive revealtion of response in order unhampered into media. A new AES algorithm proposed to prevent side channel attack aligned with attacker unit is Rijndael algorithm. In AES, the text which has been encrypted will be subjected to few rounds of encryption with the key and the same key approves the decryption of folder. An advanced higher performance method has been proposed to overcome the side channel attack.

Keywords — Side channel attack, AES algorithm, Cloud Computing, Rijndael algorithm, openstack