Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 535 – 542

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Security Algorithms for Cloud Computing

Akashdeep Bhardwaj[a*], GVB Subrahmanyam[b], Vinay Avasthi[c], Hanumat Sastry[d]

[a]*University of Petroleum and Energy Studies, Bidholi Dehradun 248001, India*
[b]*Tech Mahindra, Infocity, Hyderabad 500081 India*
[c]*University of Petroleum and Energy Studies, Bidholi Dehradun 248001, India*
[d]*University of Petroleum and Energy Studies, Bidholi Dehradun 248001, India*

Abstract

With growing awareness and concerns regards to Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms into data systems and processes. This paper presents a brief overview and comparison of Cryptographic algorithms, with an emphasis on Symmetric algorithms which should be used for Cloud based applications and services that require data and link encryption. In this paper we review Symmetric and Asymmetric algorithms with emphasis on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Cryptography, Security Algorithm, Symmetric, Asymmetric, RSA, RC6, AES, 3DES, MD5

1. Introduction

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of an eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents. In simple terms, Cryptography [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence

* Corresponding author. Tel.: +91-987-327-6660.
E-mail address:Bhrdwh@yahoo.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.215

of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text [2] and then performing decryption which is reverting back to the original plain text. With this ability, Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
- Authentication for determining whether someone or something is, in fact, who or what it is declared to be.
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
- Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

Fig 1: Encryption and Decryption process

In pure science terms [3], Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key}

Defining some terms used in Cryptography:

- Plaintext is the original intelligible source information or data that is input to algorithms
- Cipher text is the scrambled message output as random stream of unintelligible data
- Encryption Algorithm substitutes and performs permutations on plain text to cipher text
- Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text
- Keys are used as input for encryption or decryption and determines the transformation
- Sender and Recipients are persons who are communication and sharing the plaintext

With respect to Cloud computing, the security concerns [4] are end user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud:

- Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
- Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
- Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
- Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
- User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

Security Algorithms are classified broadly as:

- Private Key / Symmetric Algorithms: Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.