Advances in Computational Research
ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, 2015, pp.-243-245.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000187

A REVIEW OF CLOUD COMPUTING AND SECURITY ALGORITHMS

JADHAV U.R.*

Rajarshi Shahu Institute of Management, Aurangabad - 431 001, MS, India
*Corresponding Author: Email- ushajadhav1@gmail.com

Received: December 18, 2014; Revised: January 05, 2015; Accepted: January 15, 2015

Abstract- Cloud computing is emerging technology which uses hardware and software to provides IT services to the customer over the network. This paper discussed issues related to security of cloud storage and which algorithm are used for security of cloud. Cloud stores large amount of data from different distributed resources and it gives facility to customer easy access of data anywhere at any place, so there is need to protect data from unauthorized access and from modification data. This paper specially focused on cryptographic algorithms for the security of cloud.

Keywords- Cloud computing, Services, security, cryptography algorithm.

Citation: Jadhav U.R. (2015) A Review of Cloud Computing and Security Algorithms. Advances in Computational Research, ISSN: 0975-3273 & E-ISSN: 0975-9085, Volume 7, Issue 1, pp.-243-245.

Introduction

Cloud computing is an internet based computing which provides infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). To secure data storage, databases hosted by cloud provider it use security algorithms to maintain the confidentiality, and integrity, availability of data. It has four deployments model that are Private cloud, Public cloud, Community cloud and hybrid cloud.

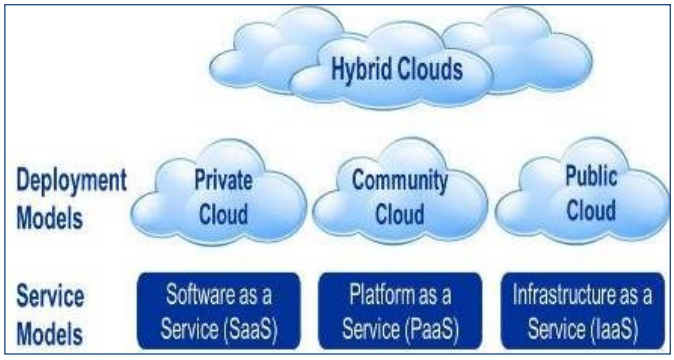

Fig. 1- Cloud Computing Model

Public Cloud: Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure, for example public cloud is IBM's blue cloud.

Private Cloud: Private cloud is cloud infrastructure dedicated to a particular organization. It is not shared with other organizations.

Community Cloud: Community cloud is an infrastructure shared by several organizations which support specific community.

Hybrid Cloud: Using the hybrid cloud, the organizations can transfer workloads between public and private cloud hosting without any trouble to the consumers. Examples of hybrid cloud are Microsoft Azure.

Security Issues to Cloud

Security issues for Cloud Computing focused in the SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the Cloud Computing and its environment. In addition, resource allocation and memory management algorithms have to be secure. There are so many issues regarding compliance model, uncertainty about security at all level, privacy.

Security Issues Faced by Cloud

Account Hijacking: In this process an individual's email and account related information is stolen by phishing, fraud and software vulnerabilities.

Vulnerabilities: Public and private clouds can be affected by both malicious attacks and infrastructure failures such as power outages.

Insecure Interface and APIs

Anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities etc.

Compliance: Compliance refers to an association's responsibility to work in agreement with established laws, specifications and standards.

Malicious Insiders: Malicious insiders who can be a current or former employee, a contractor, or a business partner who gains

access to a network, system, or data for malicious purposes.

DoS (Denial of Service)

DoS are the greatest security threat to cloud computing. DoS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services.

Cryptography

Cryptography can help Cloud computing for secure data storage. The cryptography algorithms are used to resolve this type of issues. These algorithms are Symmetric key, Asymmetric key algorithm and Hashing. Encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption helps to prevent from such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking.

Symmetric-Key Algorithms

Symmetric key algorithm uses the same key for encryption and decryption.

Symmetric key Algorithms includes, DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard).

Data Encryption Standard: The DES (Data Encryption Standard) is type of block cipher symmetric key algorithm. At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption.

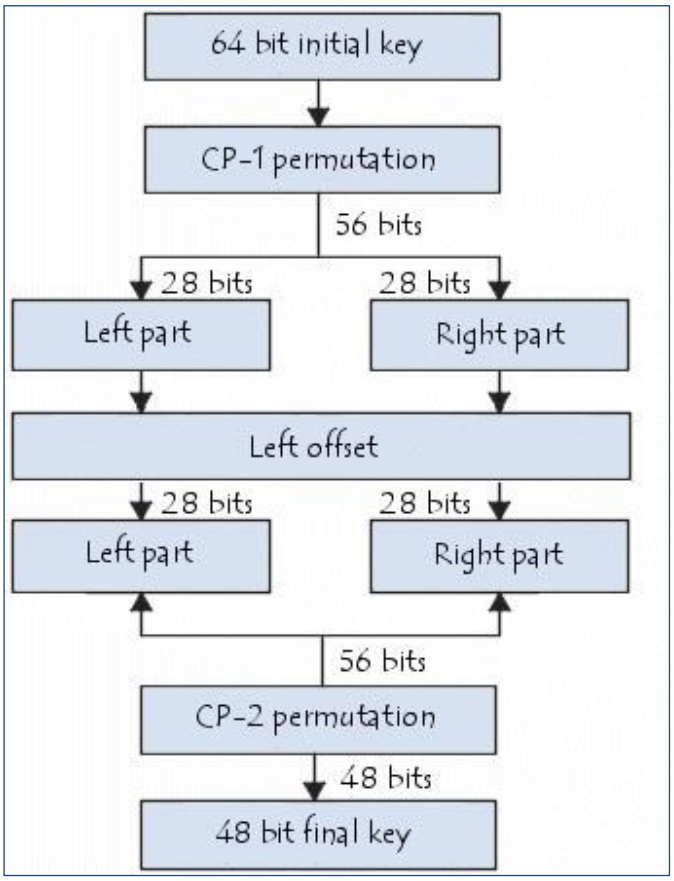

Fig. 2- DES Algorithm

Triple Data Encryption Standard (3DES): This algorithm has been designed to replace DES algorithm. It uses 3 rounds of encryption instead of one and uses 16 iterations within each round.

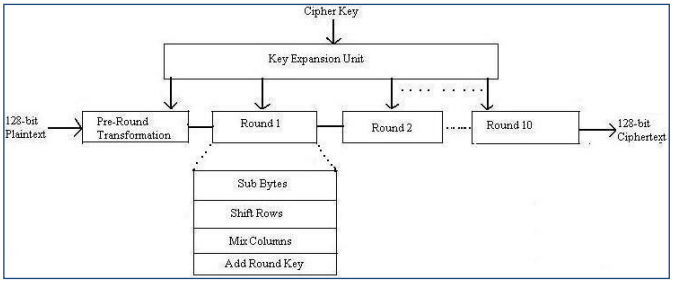

Fig. 3- Advanced Encryption Standard

Asymmetric Key Algorithm: Asymmetric encryption algorithm uses two keys private and public. These algorithm is also known as public key cryptography.

RSA Asymmetric Algorithm: RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

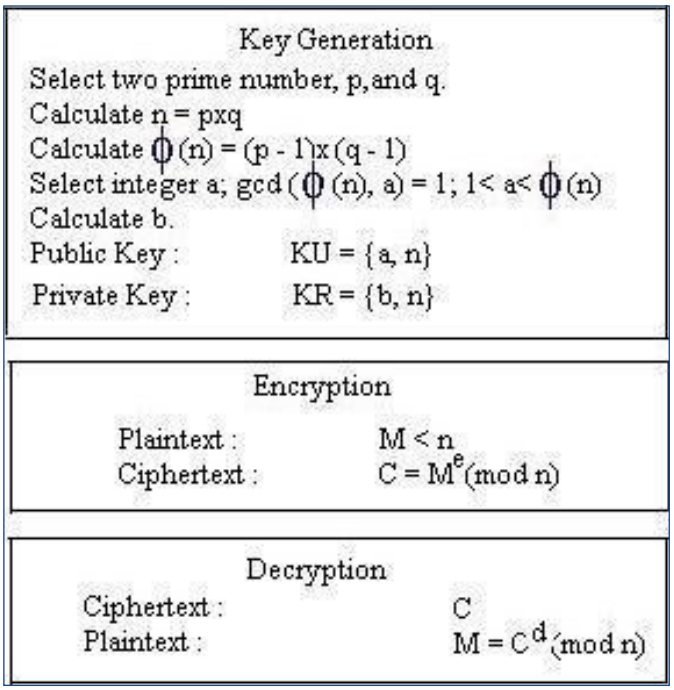

Fig. 4- Triple DES

Advanced Encryption Standard (AES): Advanced Encryption Standard is a symmetric- key block cipher. AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits.

Diffie-Hellman: Diffie-Hellman is the asymmetric encryption algorithm. It allows two users to exchange a secret key over an insecure medium without any prior secrets.

Digital Signature Algorithm: Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures.

ElGamal: The ElGamal is a public key cipher - an asymmetric key

encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement.

ECDSA: Elliptic Curve DSA (ECDSA) is a variant of the Digital Signature Algorithm (DSA) which operates on elliptic curve groups.

XTR: XTR is an algorithm for asymmetric encryption (public-key encryption). XTR is a method that makes use of traces to represent and calculate powers of elements of a subgroup of a finite field.

Conclusion

Every organization now moving their data on cloud because of the security best services provided by the cloud computing. Cloud computing gives an assuarity of confidentiality, integrity, authenticity and non-reputability. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and etc are some symmetric algorithm. RSA and Diffie-Hellman Key Exchange, Digital Signature, XTR, etc are the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms.

Conflicts of Interest: None declared.

References

[1] Nigoti R., Jhuria M. & Singh S. (2013) *International Journal of Emerging Technologies in Computational And Applied Sciences*

[2] Suresh K.S. & Prasad K.V. (2012) *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(10)

[3] Agarwal A. & Jain S. (2014) *International Journal of Computer Trends and Technology*, 9(7).