A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues

Neha Mishra[1], **Shahid Siddiqui**[2] and **Jitesh P. Tripathi**[3]

Submitted in March, 2014; Accepted in November, 2014

Abstract - Cloud computing is an emerging and revolutionary approach towards the computing and becoming more risk prone than ever before. It is an evolutionary approach of using resources and services on demand and as per need of consumers. Cloud computing providing a platform rose on the Internet for usage of IT services and flexible infrastructure to the consumers and business. Deployment and management of services or resources are maintained by the third party. Whereas there are innumerable advantages to approaching the cloud computing, it also contains various issues such as confidentiality, Integrity, Authenticity and Privacy. One of the prominent barrier to adopt the cloud computing is security. This paper comprises the elaborated study on various security issues allied to cloud computing are presented by consolidating literature reviews on cryptographic algorithms used for data security.

Index Terms – Cloud computing, Cryptographic algorithm, Decryption, Encryption, Security issue.

1.0 INTRODUCTION

Cloud computing proffering us the delivery of computing services over the Web. Cloud services providing the usage of software and hardware that are maintained and deployed by third party to the individuals or business from a remote location. A study conducted by Gartner [1,2] on Cloud Computing is regarded as the first among the top 10 most important technologies and well acknowledged by companies and organizations. Cloud computing encapsulate various services such as web mail, social networking sites, online file storage and different business application. Cloud computing enable users to access services and resources from a configurable shared pool from anywhere where network connection is available. As each users and organizations are transmigrated their information and statistics to the cloud, hence it uses the storage service of cloud deployed by cloud provider. So it is essential to secure data from any illegitimate user access or any other attack such as denial of service, modification and forgery of document etc. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. There are numerous benedictions to adopt cloud computing but still there are few loop holes that make adoption difficult to adopt. Cloud computing providers must ensure their users for hard security of data and relief from various attacks.

1.1 The following Definition of Cloud computing has been developed by NIST-

Cloud computing is a model for enable convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider inter action. Cloud model promotes availability and is composed of five essential characteristics, four deployment models and three service models.

1.2 Essential Characteristics of Cloud Computing

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

1.3 Cloud Service Models

The three fundamental classifications are often referred to as the "SPI Model" where 'SPI' refers to the Software, Platform or Infrastructure (as a Service), respectively.

1.3.1 Cloud Software as a Service (SaaS): In this type of model complete application is provided to the cloud users. It is mainly accessed through web portal and services oriented architecture (SOA).The Main Consistence Server (MCS) and Domain Consistence Server (DCS)[4].

1.3.2 Cloud Platform as a Service (PaaS): Paas encapsulate environment for the development and provisioning of cloud applications. **Examples**: Force.com, Google App Engine and Microsoft Azure.[4]

1.3.3 Cloud Infrastructure as a Service (IaaS): Infrastructure layer is used to essential IT resources. Examples: Amazon Elastic Cloud, Computing (EC2), Amazon S3 and Go Grid. [4]

1.4 Cloud Deployment Models:

- Public Cloud-Microsoft Azure, Google App Engine [4]
- Private Cloud-Eucalyptus Systems [4]

[1] *CSE, Integral University, Lucknow, India*
[2] *Asst. Professor CSE, Integral University, Lucknow, India*
[3] *Associate Professor, S R Group of Institutions, Lucknow, India,*
E-mail: [1]nehabtcs@gmail.com, [2]shahilsiddiqui@gmail.com and [3]jiteshmaths@gmail.com

- Community Cloud -Face book [4]
- Hybrid Cloud -Amazon Web Services (AWS). [4]

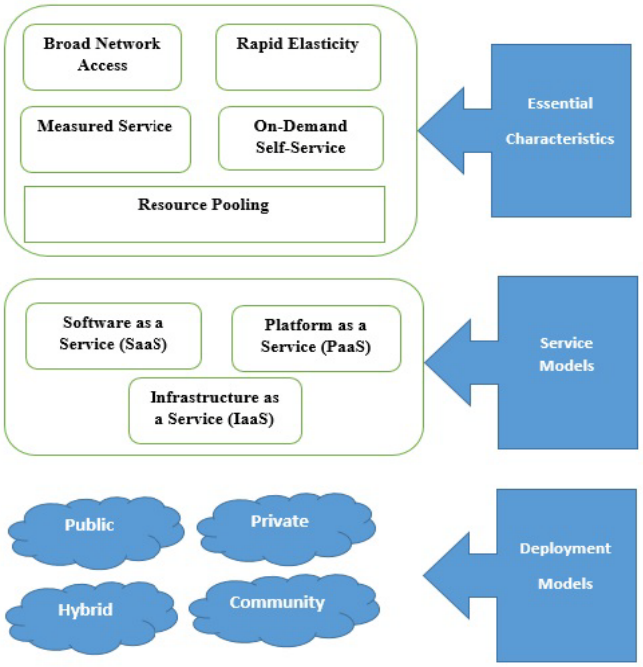


Figure 1: NIST Visual Model of Cloud Computing Definition [4]

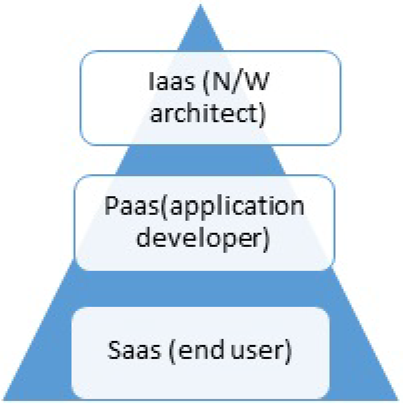


Figure 2: Cloud service model

2.0 SECURITY ISSUES AND THREATS OF CLOUD

Write correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices [5]. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven[6] while the Cloud Security Alliance identifies fourteen areas of concern[7]) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues [8].

2.1Security concern of cloud users -

2.1.1 Data- Data is main entity of communication and it must be secure enough so that it cannot be hamper by any unauthorized user. Data security should provide to the cloud users by the cloud providers. Other concern is related to the accessing of data and resources. Cloud provider must keep eye on who is accessing data, from where this activity is taking place and what type of control are applied. Data must be classified for efficient accessing of data.

2.1.2 Training of cloud users-employee or users must be trained so that they can efficiently and properly access data. Employee must be trained to know how to maintain data.

2.1.3 Service Level Agreement (SLA)–SLA is an agreement between the cloud users/business and the cloud service providers to assure which services are used by an individual user. SLA must be unambiguous or clear.

2.2 Basic Security issues for cloud

- Availability
- Data /System Integrity
- Authentication
- Storage, Backup and Recovery of data
- Data Confidentiality and privacy
- Access control

2.3 Different Threats in Cloud Computing [9]

- Account or Service hijacking
- Denial of service
- Data Scavenging
- Data Leakage
- VM escape and hopping
- Customer data manipulation
- Sniffing/Spoofing
- Attack against Web Services
- Man-in-middle attack

3.0 CRYPTOGRAPHIC ALGORITHMS FOR DATA SECURITY

In cloud computing data security is the main concern. For the same different cryptographic algorithms are used. Original text message is known as plaintext and the coded form is known as cipher text. Conversion of plaintext to cipher text is called encryption. Cipher text can be converted back to plain text, this is call decryption. Cryptography comprises the study of encryption and decryption.

3.1 Symmetric encryption is a technique to camouflage the originality of contents of blocks or streams with message file, encryption key and password. Single key is used to encrypt or decrypt data. There are two kinds of symmetric-key encryption algorithms are used to wrap-up the content in a mask i.e. Block cipher and Stream cipher. In block cipher a block of plain text of fixed size is encrypted at a time using key. In stream cipher a bit of stream is encrypted at a time using key. e.g. DES, AES, triple DES, Blowfish etc. are cloud computing algorithms.

3.1.1 DES –DES is a symmetric algorithm for data encryption by using 56 bit key size. It uses balanced feistal structure. It is designed by IBM in 1977.DES uses 64 bit block. Feistal function for this are – expansion, substitution, key mixing and permutation and for the encryption process of DES there are two permutations, one is initial and the other is final permutation and sixteen Feistel rounds are used to generate the key, for each round 48-bit keyis generated from the cipher key.[9,10].

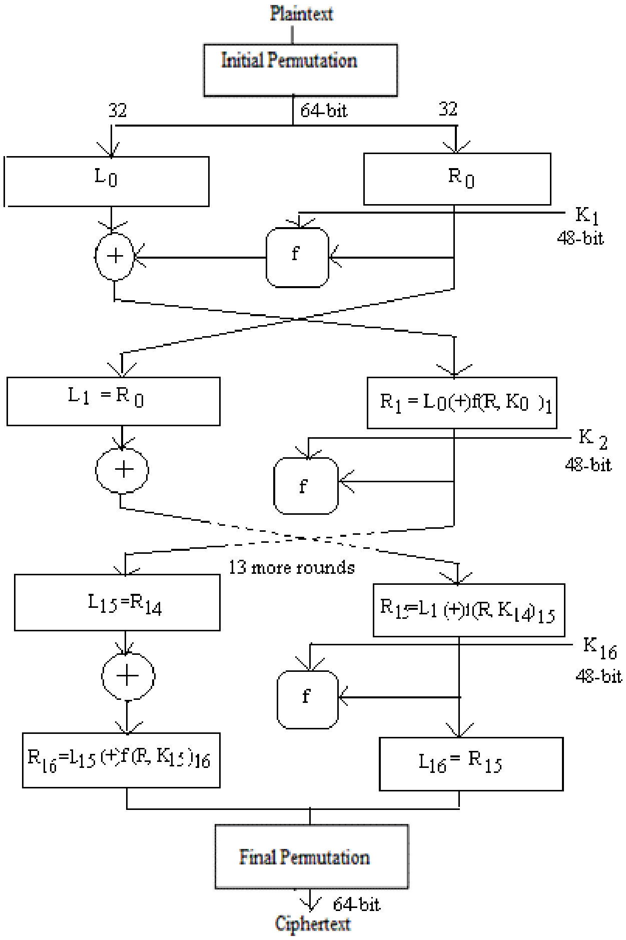


Figure 3: Encryption with DES

3.1.2 3DES- This encryption algorithm is derived from DES. It provides an easy and efficient way of increasing the key size of DES to protect against brute force attack.[9,10]

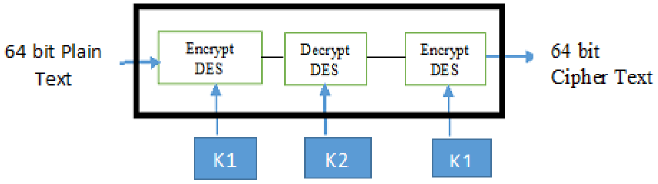


Figure 4: Encryption with 3DES

3.1.3 AES – AES is a symmetric algorithm for data encryption by using 128, 192, 256 bit key. This algorithm is affected by Brute force attack. Because it uses 128 bit block size it more secure than any other algorithm.[9,10]

3.1.4 RC-5-RC-5 encryption technique is Designed by Ronald Rivest in 1994.This symmetric algorithm uses Keysize of 0-2040bit and uses variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255).It is susceptible to 64-bit blocks differential attack using 2^{44} chosen plaintexts. [9,10]

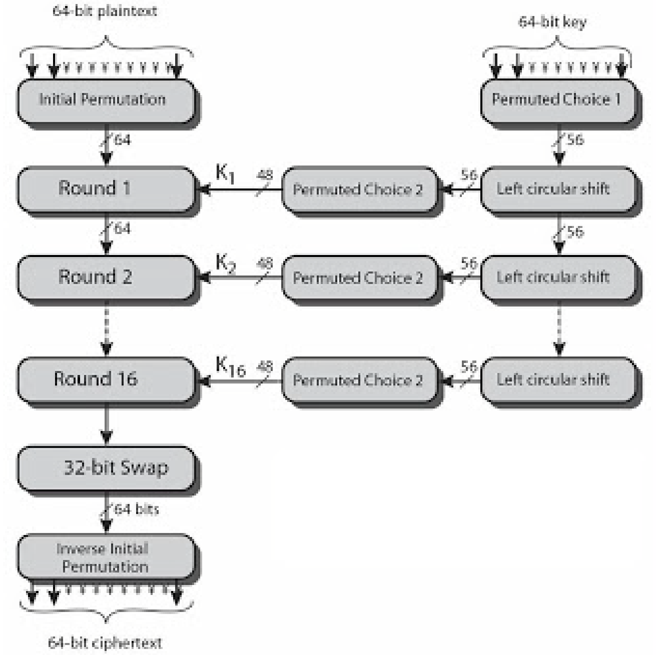


Figure 5: Encryption with AES

3.1.5 IDEA-This block cipher uses 64 bits block of message and 128 bit key. This encryption algorithm suffer from narrow bicliques attack.[9,10]

3.1.6 BLOWFISH-Blowfish is one of the block cipher algorithm for encryption. This encryption technique uses the same secret key to both encryption and decryption of information. Blowfish uses 64 bit block size and variable length key, from 32 bits to 448 bits. Blowfish is appropriate technique for applications where the key is not changed frequently. Over the 32-bit microprocessors it is faster and efficient than other encryption techniques with huge data. It uses 16-round Feistel network.[9,10]

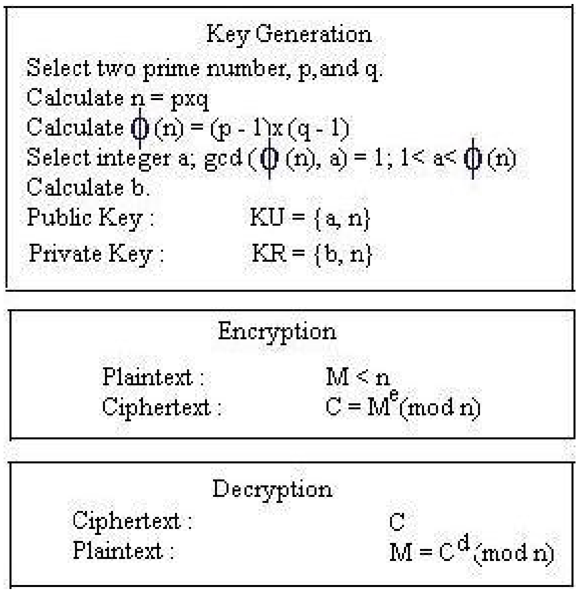
3.2 Asymmetric encryption is used to encrypt small block of data. One key is used to encrypt data or other key is used to decrypt data. Two keys are: Private Key and Public Key. The Public key is used by the sender for the purpose of encryption and the private key is used for the purpose of decryption of data by the receiver. In cloud computing these algorithms are used to generate keys. Some of the common asymmetric-key algorithms for cloud are: RSA,DH and IKE.

3.2.1 RSA- RSA is a public key cryptographic algorithm for data security. This is a most common encryption algorithm used by people to encrypt message with two keys. RSA algorithm encryption and decryption is based on the modular exponential and has two exponents, a and b, where a is used for public and b is used for private. Let the plaintext is M and C is cipher text, then at encryption.[9,10]

C =Ma mod n

And at decryption side

M = Cb mod n.



Key Generation

Select two prime number, p,and q.

Calculate n = pxq

Calculate ϕ (n) = (p - 1)x (q - 1)

Select integer a; gcd (ϕ (n), a) = 1; 1< a< ϕ (n)

Calculate b.

Public Key :	KU = {a, n}
Private Key :	KR = {b, n}

Encryption

Plaintext :	M < n
Ciphertext :	C = M^e(mod n)

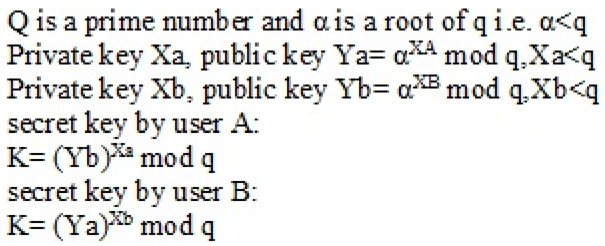
Decryption

Ciphertext :	C
Plaintext :	M = C^d(mod n)

Figure 6: RSA algorithm

3.2.2 Diffie-Helman Key Exchange- This is created by the Whitfield Diffie and Martin Hellman In 1976.This algorithm depends on the complexity of discrete logarithm. Diffi-hellman basically used for key exchange between two users.[9,10].

ALGORITHM:



Q is a prime number and α is a root of q i.e. α<q

Private key Xa, public key Ya= α^{XA} mod q,Xa<q

Private key Xb, public key Yb= α^{XB} mod q,Xb<q

secret key by user A:

K= $(Yb)^{Xa}$ mod q

secret key by user B:

K= $(Ya)^{Xb}$ mod q

3.2.3 ElGamal- This is an asymmetric algorithm used for transmitting digital signatures as well as for key exchange. El Gamal is based on the applicability of discrete logarithms. It is rely on the logarithmic number’s characteristics or calculations of these numbers. [9,10]

4.0 COMPARISON AND RESULT

Different symmetric algorithms are compared below on the basis of design feature. Analysis and performance Comparison Table of Asymmetric encryption algorithm-[9,10,12]

Larger the block size means greater security but decreases the encryption/decryption speed. AES has larger block size among the entire algorithms and has greater security capability than other.

Table 1: Comparison of Cryptographic Asymmetric encryption algorithms

DESIGN FEATURE	ASYMMETRIC ALGORITHM			
	RSA	DIFFIE-HELLMAN	ElGamal	ECC
SECURITY	Based on the problem of factoring large Numbers	Vulnerable and secure against eavesdropping	Bases on the discrete logarithm	Based on difficulty to determine secret key k given kP and p
STANDARD	Free for all, Patented only in US	ANSI X9.42	FIPS186-3	IEEE P1363
USAGE	Used for confidentiality and key exchange as well as for digital sign.	Used for Key exchange	Used for both encryption and DSA	Implementing algorithm such as DSA
NO. OF KEYS	2	2	2	2
KEY LENGTH	512 to 15,360	2013,224 bits for q and 2048 bits for p	2048 bit	112 bit to 512 bit
ATTACKS	Brute forced and oracle attack etc.	Denial of service attack	Chosen cipher text and malleability	Timing or simple and differential power attack (side channel 0r fault)

Larger the key size means greater security but decreases the encryption/decryption speed .Blowfish has larger key length among other algorithm.

No. of rounds, multiple rounds offers greater security. Blowfish has 16 rounds which is typically a standard number of rounds.

The most important thing no attack is known to be successful against Blowfish. Hence Blowfish is superior to other algorithms.

Different asymmetric algorithms are compared below on the basis of design feature. Analysis and performance Comparison Table of symmetric encryption algorithm-[9,10,12].

Table 2: Comparison of cryptographic symmetric encryption algorithms

SYMMETRIC ALGORITHM	**DESIGN FEATURE**					
	BLOCK SIZE	**KEY SIZE**	**NO. OF ROUNDS**	**NETWORK**	**ATTACK**	**POSSIBLE KEYS**
AES	128	128,192,256	10,12,14	Non-Feistal	BruteForce	2^{128},2^{192}, 2^{256}
3DES	64	168,112 or 56	48	Feistal	Theoretical meet-in-the middle attack	2^{168} 2^{112} 2^{56}
IDEA	64	128	8.5	Lai-massey scheme	Narrow-biclique	2^{128}
RC-5	32,64,128 (64 suggested)	0-2040 (128 suggested)	1-255 (12 suggetsed)	Feistal	Differential	2^{128}
BLOWFISH	64	Variable length (32-448)	16	Feistal	No attack is known but suffering from weak key	2^{32},2^{448}

ECC have advantage over RSA i.e.: requirement of less memory and computation time. Advantages of ECC compared to RSA increases abruptly because of length of the key. While RSA need to double its key size, ECC requires few Bit to obtain the same level of security. The RSA currently changes its key size to 2048 Bit and ECC only need to increase its key size to 192 Bit.ECC devices occupies less storage, less power, less memory, and less bandwidth in compare to other systems. Thus ECC has computational advantages with shorter key size than SA.RSA is most widely used algorithm for encryption and key exchange. ElGamal is extended and updated version of DH.

5. 0 CONCLUSION

Cloud computing is an innovative computing trend and many organizations and business are shifting towards the cloud but there are certain barrier to adopt the services. The major reason to avert the usage of cloud is security. There are many cryptographic algorithms that can be deployed over the cloud to provide the security.

DH and ElGamal accept the variants of elliptic curve.RSA is faster in encryption and slower in decryption to ElGmal and half of DH. Hence RSA is efficient among all other asymmetric algorithms.

RSA and Diffie-Hellman Key Exchange both are asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange algorithms generate encryption keys for symmetric algorithms.

DES and AES are frequently used symmetric algorithms.DES algorithm is easy to implement then AES. In terms of Security of data, Flexibility, Memory usage, and performance AES (Rijndael) is best among all.

AES effective in both software and hardware.3DES and DES are slow in software. Blow fish is more efficient in software. AES is excellent in security rate and execution time than RSA.

This paper encompasses a theoretical performance analysis of symmetric or asymmetric encryption algorithm.

In the future, our research will be extend by providing implementation of algorithm.

6.0 REFERENCES

[1]. Vanya Diwan, Shubhra Malhotra, Rachna Jain, “Cloud Security Solutions: Comparison among Various Cryptographic Algorithms”,IJARCSSE , April 2014.

[2]. [Gartner Inc, “Gartner identifies the Top 10 strategic technologies for 2011”. Online Available: http://www.gartner.com.

[3]. David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez, “An analysis of security issues for cloud computing Keiko Hashizume1”.

[4]. .M. Vijayapriya, “SECURITY ALGORITHM IN CLOUD COMPUTING: OVERVIEW”, International Journal of Computer Science & Engineering Technology (IJCSET),2013.

[5]. "4 Cloud Computing Security Policies You Must Know". Cloud Computing Sec. 2011.

[6]. Gartner, “Seven cloud-computing security risks".

[7]. Cloud Security Alliance. 2011, "Security Guidance for Critical Areas of Focus in Cloud Computing”.

[8]. "Cloud Security Front and Center". Forrester Research. 2009-11-18.

[9]. Hashizume , “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications 2013.

[10]. Rashmi, “A Survey of Cryptographic Algorithms for Cloud Computing”. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS),2013.

[11]. EloffM.M, Smith E., “The management of security in Cloud computing”, Univ. of South Africa, Pretoria, South Africa,2013.

[12]. Maulik P. Chaudhari and Sanjay R. Patel, “A Survey on Cryptography Algorithms”, IJARCSMS, 2014.