Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.517 – 525

RESEARCH ARTICLE

Security in Cloud Computing Using Cryptographic Algorithms

Miss. Shakeeba S. Khan[1], Miss. Sakshi S. Deshmukh[2]

[1],[2]Department of Computer Sci. & Engg., PRMIT&R Amravati, India
[1] khanshakeeba123@gmail.com; [2] ssdeshmukh18@gmail.com

Abstract— ***Cloud computing is the concept implemented to decipher the Daily Computing Problems. Cloud computing is basically virtual pool of resources and it provides these resources to users via internet. Cloud computing is the internet based development and used in computer technology. The prevalent problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). In this paper we analyses different security issues to cloud and different cryptographic algorithms adoptable to better security for the cloud.***

Keywords— ***Cloud Computing, Cryptographic Algorithm, Internet, Security Algorithms, Security Attacks, Security Issue***

I. INTRODUCTION

Cloud computing is the concept of using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

II. TYPES OF CLOUDS

There are basically four types of clouds, which are described below

A. *Public Cloud*

This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-perusage model.

B. *Private Cloud*

This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

C. *Community Cloud*

This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

D. *Hybrid Cloud*

This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

III. CHARACTERISTICS OF CLOUD COMPUTING

There are several characteristics of cloud computing, which are described below

A. *Virtualization*

Through Cloud computing, user is able to get service anywhere through any kind of terminal. User can attain or share it safely anytime.

B. *High Reliability*

Cloud uses data fault tolerant to ensure the high reliability of the service.

C. *Versatility*

Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

D. *On Demand Service*

Cloud is a large resource pool that a user can buy according to his/her need; cloud is just like running water, and gas that can be charged by the amount that user used.

E. *Extremely Inexpensive*

The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully take advantage of low cost.

IV. SECURITY ISSUES TO THE CLOUD

The security requirements of a cloud and non-cloud data center are fairly similar. The Cloud Security Alliance's initial report contains a different sort of taxonomy based on different security domains and processes that need to be followed in general cloud deployment. Some privacy and security-related issues that are believed to have long-term significance for cloud computing are

A. *Governance*

Governance implies management and oversight by the organization over procedures, standards and policies for application development and data technology service acquirement, also because the style, implementation, testing, use, and watching of deployed or engaged services.

B. *Compliance*

Compliance refers to an association's responsibility to work in agreement with established laws, specifications and standards. One with all the foremost common compliance problems facing a company is information location means storage of data or information.

C. Malicious Insiders

This threat is well known to most organizations. ‘Malicious insiders’ impact on the organization is considerable. Malicious insiders are the threat which has access to the data or information about the organization being a member of the organization. As cloud consumers application data is stored on cloud storage provided by cloud provider which also has the access to that data.

D. Account or service Hijacking

This threat occurs due to phishing, fraud and software vulnerabilities. In this type attacker can get access to critical areas onto the cloud from where he can take permit and steeling important information leading to compromise of the availability, integrity, and also confidentiality to the services.

E. Hypervisor vulnerabilities

The Hypervisor is the main software component of Virtualization. There known security vulnerabilities for hypervisors and solutions are still limited and often proprietary.

F. Insecure 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 security threats may occur to organizations if the weak set of interfaces and APIs are used.

V. CRYPTOGRAPHY

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day’s cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host [2], and cryptography can resolve these issues to some extents. Consider an example, In the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data. This will helps us in reduction of Virtualization vulnerability. For secure communication between the host domain and the guest domain, or from hosts to management systems, 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 will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking [5].

A. Symmetric Key Algorithms

The most important type of the encryption is the symmetric key encryption. Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption [1]. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of a symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit at a time is encrypted. Some popular Symmetric-key algorithms used in cloud computing are: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

1) Data Encryption Standard (DES): The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, 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. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure 1.

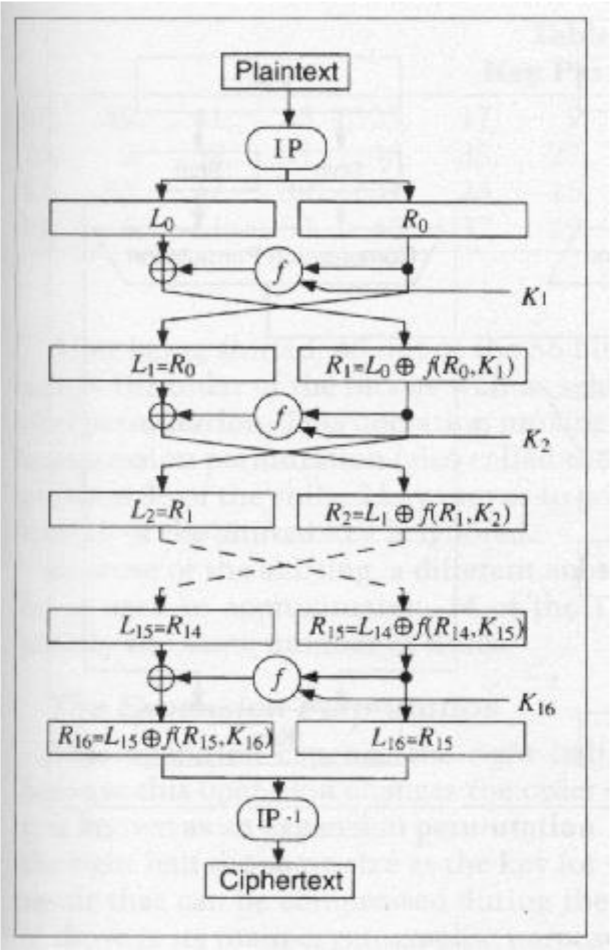

Plaintext
IP
L_0
R_0
f
K_1
$L_1=R_0$
$R_1=L_0 \oplus f(R_0,K_1)$
f
K_2
$L_2=R_1$
$R_2=L_1 \oplus f(R_1,K_2)$
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus f(R_{14},K_{15})$
f
K_{16}
$R_{16}=L_{15} \oplus f(R_{15},K_{16})$
$L_{16}=R_{15}$
IP^{-1}
Ciphertext

Fig. 1 Encryption with DES

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

2) Advanced Encryption Standards: Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). 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. AES operates on a 4×4 column-major order matrix of bytes, known as the state. Encryption with AES is shown in figure 2.

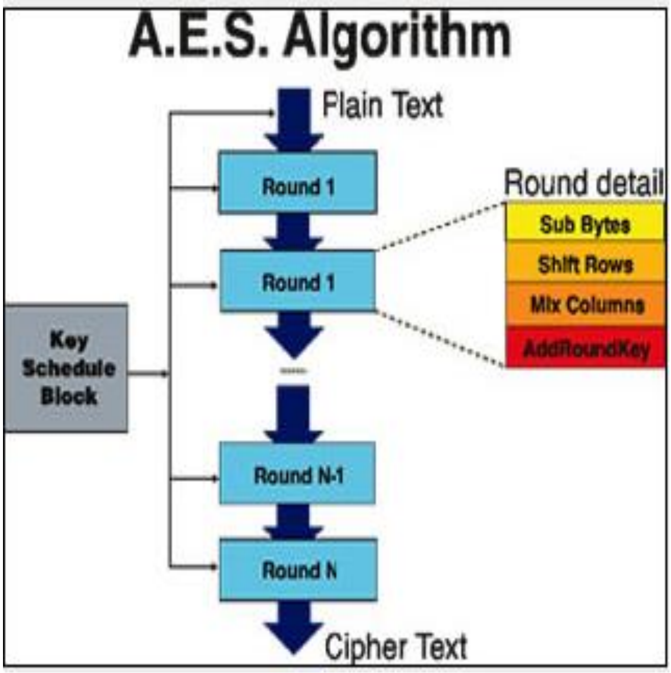


Fig. 2 Encryption with AES

3) Triple DES: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against attacks, without the need to design a completely new block cipher algorithm. Many former DES users can use Triple DES (TDES) which was described and analyzed by one of DES's patentees. It involves applying DES three times with two (2TDES) or three (3TDES) different keys as shown in figure 3. TDES is quite slow but regarded as adequately secure.

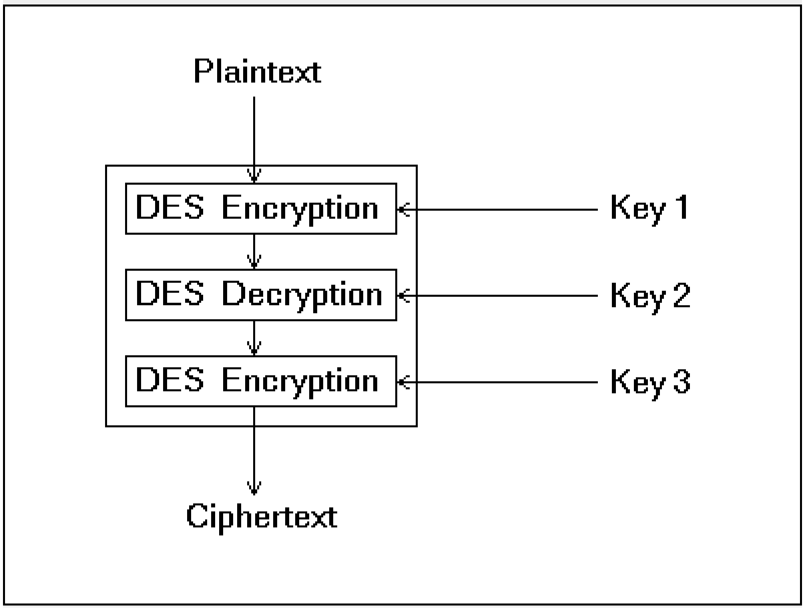


Fig. 3 Encryption with Triple DES

4) Blowfish Algorithm: Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches. Data encryption happens via a 16-round Feistel network [12] as shown in figure 4.

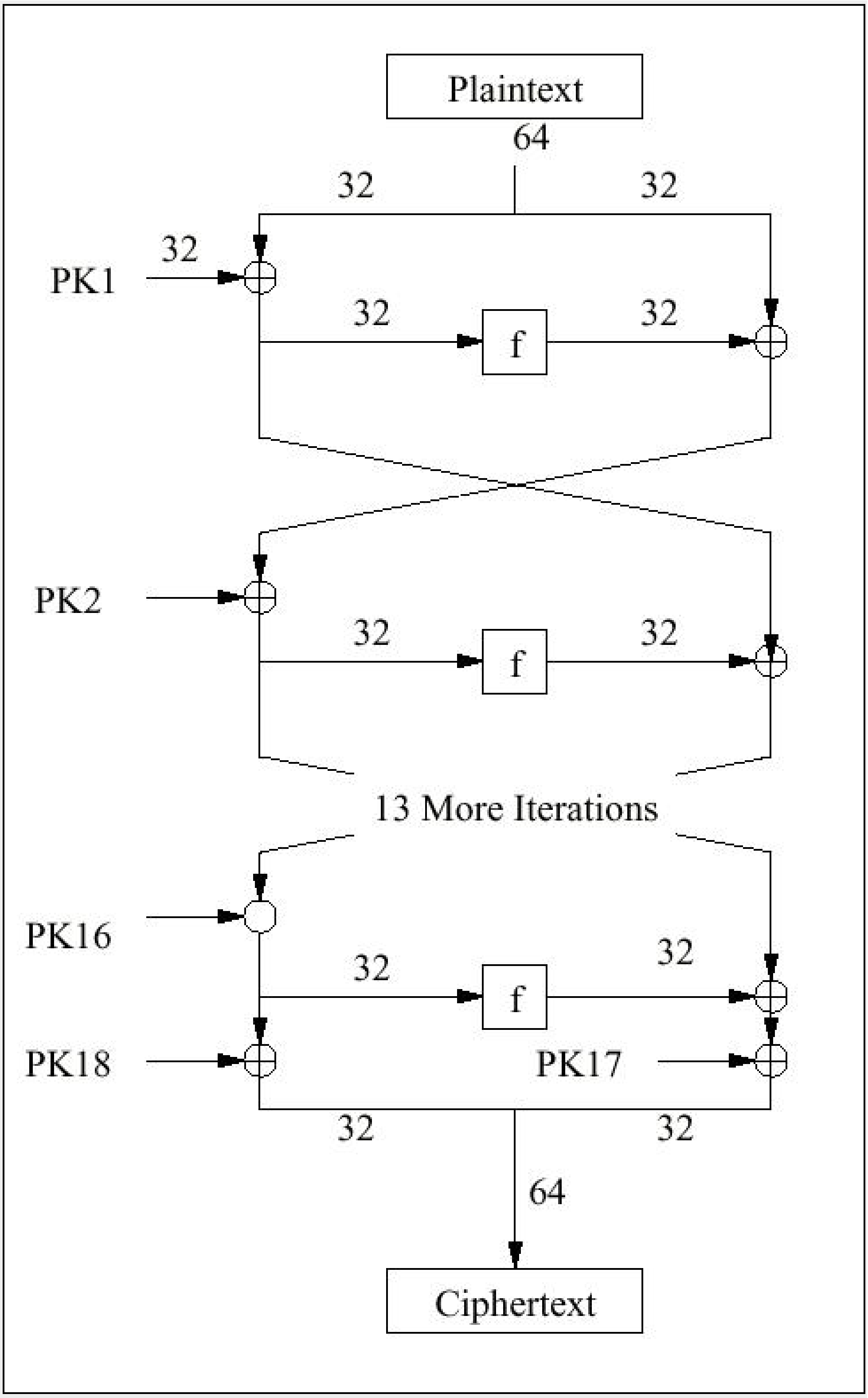


Fig. 4 Encryption with Blowfish Algorithm

B. Asymmetric Key Algorithm

Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA, IKE, Diffie-Helman Key Exchange.

1) Homomorphic Encryption: Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services. Cloud consumer encrypts its data before sending to the Cloud provider, But, each time he has to work on that will have to decrypt that data. The consumer will require giving the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud. Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption (without knowing the private key); only the consumer will have the secret key. When we decrypt the result of any operation, it is the same as if we had performed the calculation on the plaintext (or original data). The Homomorphic encryption is distinguishing, according to the operations that are performed on raw data [9].

- Additive Homomorphic encryption: additions of the raw data.
- Multiplicative Homomorphic encryption: products for raw data.

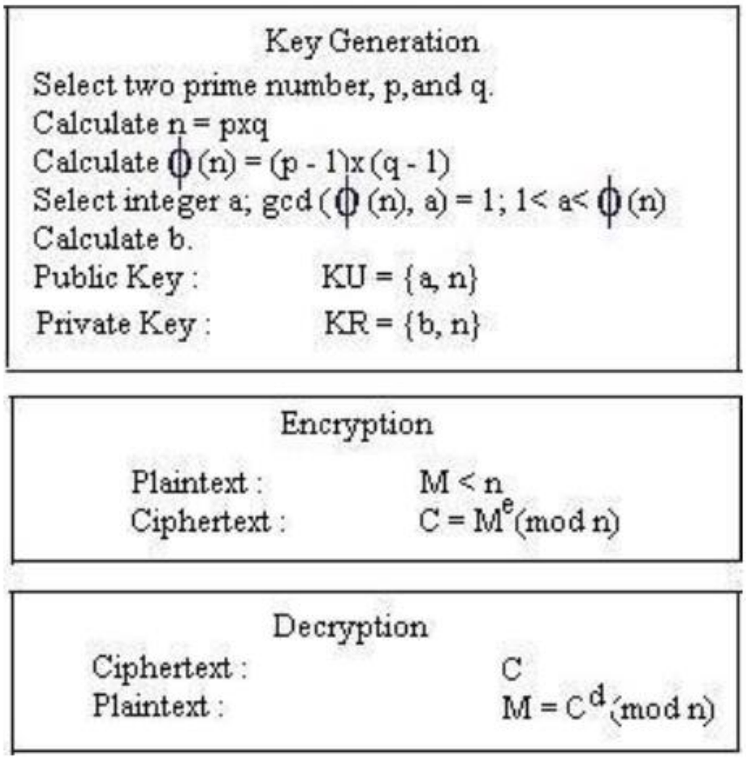
2) RSA: RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption [9]. Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption.

$$C = P^a \bmod n$$

And at decryption side

$$P = C^b \bmod n$$

n is a very large number, created during key generation process. The process is shown in figure 5.



Key Generation

Select two prime number, p,and q.

Calculate $n = pxq$

Calculate $\phi(n) = (p - 1)x(q - 1)$

Select integer a; $\gcd(\phi(n), a) = 1$; $1 < a < \phi(n)$

Calculate b.

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

Encryption

Plaintext :	$M < n$
Ciphertext :	$C = M^e (\bmod n)$

Decryption

Ciphertext :	C
Plaintext :	$M = C^d (\bmod n)$

Fig. 5 RSA Algorithm

3) Diffie-Hellman Key Exchange: In 1976, Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will set up a secret key to their symmetric key system, using an insecure channel. To set up a key Alice chooses a random integer a Є [1; n] computes g^a , similarly Bob computes g^b for random b Є [1; n] and sends it to Alice. The secret key is gab, which Alice computes by computing $(g^b)^a$ and Bob by computing $(g^a)^b$. The important concepts on which the security of the Diffie-Hellman key exchange protocol depends are [11]:

- Discrete Logarithm Problem (DLP): If from g and g^a Eve, an adversary can compute a, then he can compute g^{ab} and the scheme is broken.
- Diffie-Hellman Problem (DHP): If from given the information g, g^a and g^b with or without solving the discrete logarithm problem, Eve can compute g^{ab} then the protocol is broken. It is still an open problem if DHP is equivalent to DLP.
- Decision Diffie-Hellman Problem (DDH): If we are given g; g^a; g^b and g^c, DDH is to answer the question, deterministically or probabilistically, Is ab = c mod n?

VI. Conclusions

Cloud computing is a newly emerging thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud.

DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithm. DES and AES are mostly used symmetric algorithms. DES is quite simple to implement then AES. RSA and Diffie-Hellman Key Exchange are the asymmetric algorithms.

These security algorithms are currently used in a cloud computing environment. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the environment.

References

[1] AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms" International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.

[2] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.

[3] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing", VSRD International Journal of CS & IT Vol. 2 Issue 3, 2012, pp. 242-249.

[4] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing",Springer Journal of Cloud Computing: Advances, Systems and Applications 2012.

[5] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.

[6] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Companies, Inc., New York, Special Indian Edition 2007.

[7] Wayne Jansen and Timothy Grance "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, Special Publication 800-144, December 2011, 80 pages

[8] Akhil Behl "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.

[9] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering Volume I, July 4 - 6, 2012, London, U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online).

[10] Cloud Security Alliance "Security Guidance for critical Areas of Focus in cloud computing V3.0", 2011, 177 pages.

[11] Ayan Mahalanobis "Diffie-Hellman Key Exchange Protocol,Its Generalization and Nilpotent Groups.", August 2005, 40 pages.

[12] G. Devi , M. Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803,2012, pp. 592-596.

[13] Mandeep Kaur and Manish Mahajan "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2 N o. ISSN No. 2231-2471 (Online) , 2319-2224 (Print), 10 October 2012, pp.831-835.

[14] Leena Khanna, Prof. Anant Jaiswal "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them", International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp. 279-283.

[15] Armbrust, Fox, Griffith, Joseph, "*Above the clouds: A Berkeley view of cloud computing*"[2009].

[16] Buyya, Venugo, "*Cloud Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th Utility*", [2008].

[17] Caceres, Lindner, Vaquero, "*A break in the clouds: towards a cloud definition*", [2008].