International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.353-360
http://dx.doi.org/10.14257/ijsia.2015.9.10.32

Cloud Security Algorithms

Er. Ashima Pansotra[1] and Er. Simar Preet Singh[2]

[1]*Research Scholar, DAV University, Jalandhar,* [2]*Assistant Professor, DAV University, Jalandhar*
[1]*ashimapansotra6@gmail.com,* [2]*er.simarpreetsingh@gmail.com*

Abstract

Cloud computing appear to be a very popular and interesting computing technology. Every third person is using cloud computing directly or indirectly for example e-mail, most commonly used application of cloud computing, you can access your mail anywhere anytime. Your e-mail account is not visible on your personal computer but you have to access that with the help of internet. Like e-mail cloud computing provide many other services such as storage of any kind of data, access to different applications, resources etc. So users can easily access and store data with low cost and without worrying about how these services are provided to user. Due to this flexibility everyone is transferring data to cloud. To store data on cloud user has to send their data to the third party who will manage and store data. So it is very important for the company to secure that data. Data is said to be secured if confidentiality, availability, integrity is present. To secure data we have different algorithms. In this paper we will discuss the different cryptography of algorithms.

Keywords: *Cloud computing, Cryptography, Encryption, Decryption, Cipher Text, DES, TDES, AES, RSA, Homomorphic, IDEA, Blowfish*

1. Introduction

Cloud is nothing but the group of servers and datacenters that are placed at different places and these severs and datacenters are responsible for providing on demand service to its users with help of internet. The service provided by cloud is not present on user's computer. User has to access these services with help of internet connection through subscribing them. The main advantage of Cloud computing is that it eliminates the need for user to be in same location where hardware software and storage space is physically present. Cloud makes it possible to store and access your data from anywhere anytime without worrying about maintenance of hardware software and storage space. All these services are provided to user at low cost. User has to pay according to storage space he is using. Due to this flexibility everyone is transferring his data on cloud.

Security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away [8]. While sending of data and during storage data is under threat because any unauthorised user can access it, modify it, so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorised disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorised user. Availability refers to assurance that user has access to information anytime and to any network. In the cloud confidentiality is obtained by cryptography.

Cryptography is a technique of converting data into unreadable form during storage and transmission that it appears waste to intruder. The unreadable form of data is known

ISSN: 1738-9976 IJSIA

as cipher text. When data is received by receiver it, will appear in its original form which is known as plain text. Conversion of plain text to cipher text is known as encryption and reverse of this (cipher text to plain) is known as decryption. Encryption takes place at sender's end whereas decryption takes place at receiver's end.

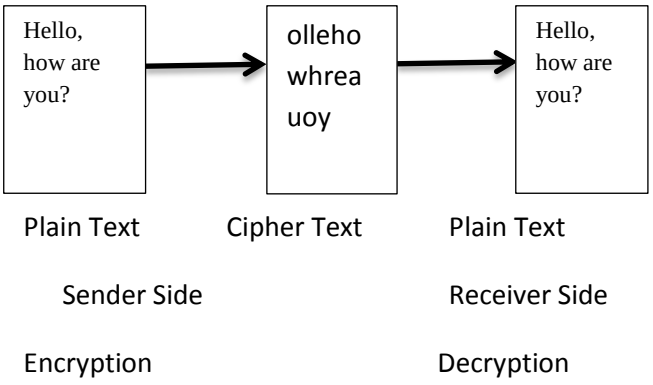

Figure 1. Encryption Decryption Process

There are three types of cryptography algorithms (i) Symmetric algorithms (ii) Asymmetric algorithms (iii) Hashing.

In hashing a fixed length signature is created with the help of algorithms or hash function for the encryption of data. Each message consists of different hash value, but the hashing has one drawback i.e. once the data is encrypted, it cannot be decrypted. This limitation of hashing was removed by symmetric and asymmetric algorithms. Symmetric algorithm is also known as "Secret Key Encryption Algorithm" in symmetric key algorithm, only one key is used for encryption and decryption i.e. private key, where as in asymmetric algorithm both public and private keys are used for encryption and decryption, asymmetric algorithm is also known as "Public Key Encryption Algorithm"[1].

2. Existing Algorithms

Many organisations and people store their important data on cloud and data is also accessed by many persons, so it is very important to secure the data from intruders. To provide security to cloud many algorithms are designed. Some popular algorithms are:-

2.1. Data Encryption Standard (DES)

DES is very commonly used symmetric key algorithm. It was developed by IBM in 1974, but now a days many methods are found that had proven this algorithm unsecured [1].

In DES algorithms block cipher is of 64 bits [2] and key used is of 56 bits out of 64 bits of key is used rest of 8 bits are padded. In block cipher we encrypt block of data which consist of plain text by combination of confusion and diffusion to make cipher block then this cipher block has to pass 16 rounds, before passing through these 16 rounds the 64 bits of data is divided into 32 bits. After dividing the data into 32 bits, F-function (Feistel function) is applied. F-function consists of substitution, permutation, key mixing. The output of function is combined with other half of the data using XOR gate alternate crossing of data is done; then crossing of data is done.

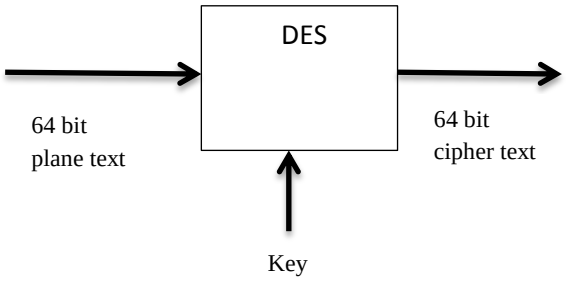

Figure 2. High Level Diagram of DES Encryption Algorithm

After doing 16 such rounds cipher text is produced or encryption of data is done. To decrypt the data reverse operation is done. The drawback of DES is that key used in DES is very small and its security can be broken easily and DES works fast on hardware only and woks slowly on software. As shown in Fig 3 data bits are divided into two parts L_f and R_f than F function and XOR operation is applied on R_f, and output is combined with L_f.

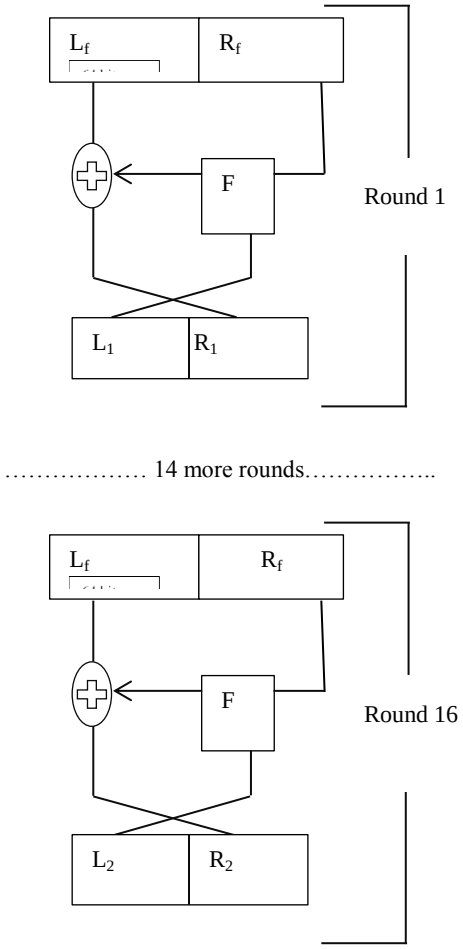

Figure 3. Inside Working of DES Algorithm

2.2. Advance Encryption Algorithm (AES)

Advance Encryption algorithm AES is also known as Rijndael. AES is announced as U.S FIPS by NIST in 2001. In AES, different size of key is used i.e. 128, 192 or 256 bits,

depends on how many cycle it uses [3]. For 10 cycles 128-bit key, 12 cycles 192 bit key and for 14 cycles 256 bit key is used. All rounds of AES are similar except the last one. AES works on 4x4 matrixes. AES consists of key expansion, initial and final round. Initial round consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and final round also consists of similar function as initial round except mix columns. AES works fast on both software and hardware.

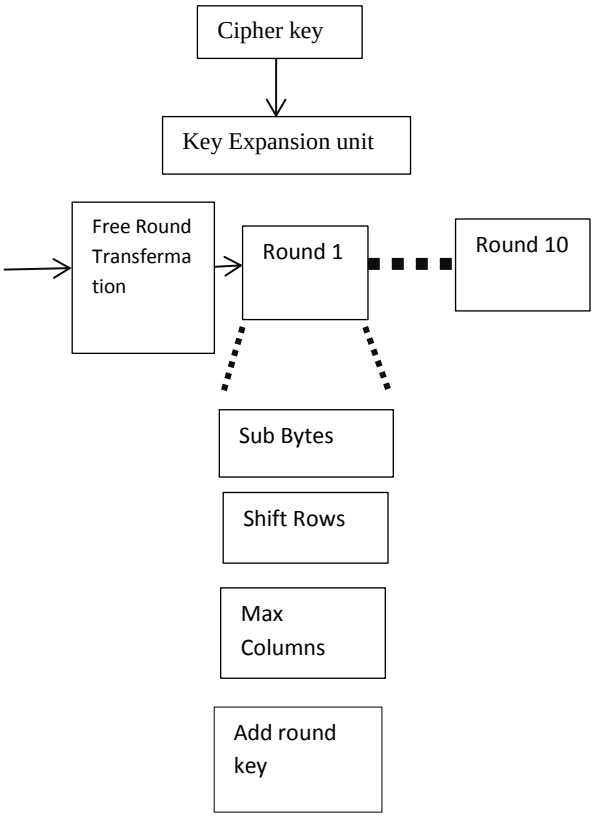

Figure 4. Encryption with AES Algorithm [13]

2.3. Triple- DES (TDES)

TDES is enhanced version of DES in TDES the key size is increased to increase i.e. 168 bits the security of data [14]. In TDES only size of key is increased rest of the working is similar to DES [12]. In TDES three different keys are applied on cipher block.

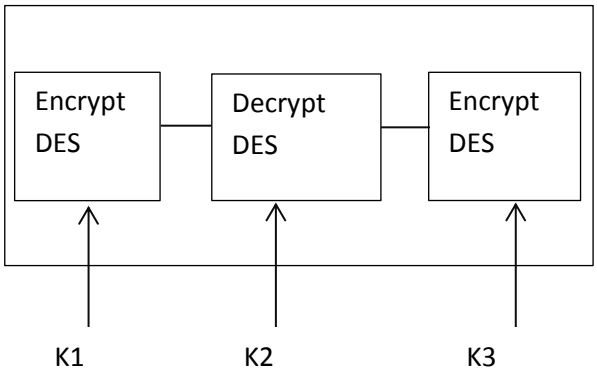

Figure 5. TDES Encryption Algorithm [13]

2.4. Blowfish Algorithm

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost similar to DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large [4] and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES [11]. Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits. One part taken as the left part of message and other is right part of message. The left part is XOR with the elements of P-array which creates some value, then that value is passed through transformation function F. The value originated from the transformation function is again XOR with the other half of the message i.e. with right bits, then $F^{|}$ function is called which replace the left half of the message and $P^{|}$ replace the right side message.

2.4. IDEA

International Data Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used. What is the sequence of operations performed in each round? Let $I_1, I_2 \ldots I6$ be the inputs to [5] round 1, functions in round 1 are:-

(i) Multiply I_1 and K_1.
(ii) Add I_2 and K_2.
(iii) Add I_3 and K_3.
(iv) Multiply I_4 and K_4.
(v) Now, step 1 is EXOR with step 3.
(vi) Step 2 EXOR with step 4.
(vii) Multiply step 5 with K_5.

Similar operations are performed in other rounds.

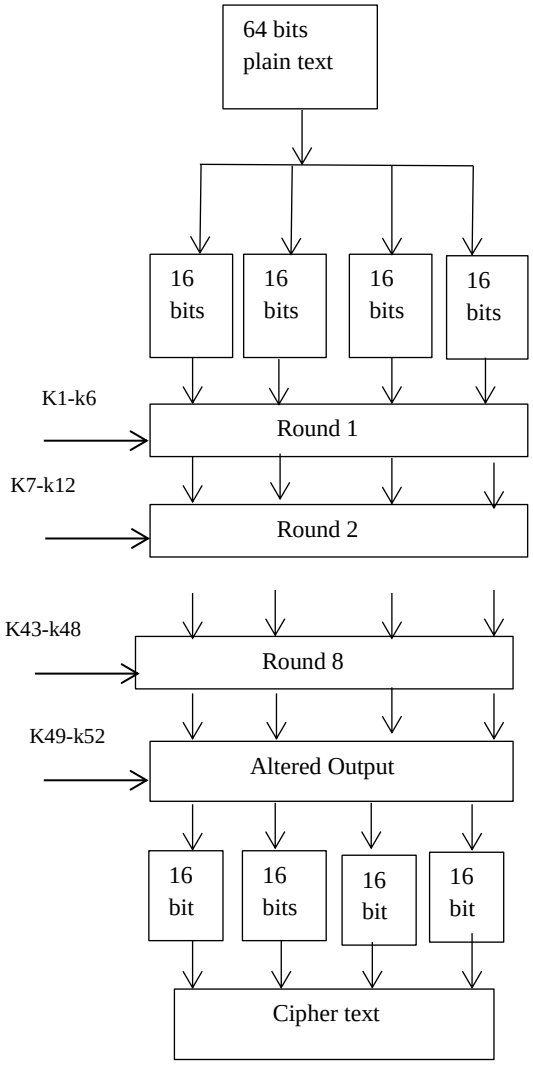

Figure 6. Encryption with IDEA

2.5. Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key [10]. In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

2.6. RSA

RSA was invented by Ranold Fivest, Adi Shamir and Leonard Adleman in 1977. [6] RSA is also an asymmetric algorithm. Functioning of RSA is based on multiplication of two large numbers. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key [9]. The two numbers that are used for multiplication-one of them is public other is private. Steps for RSA algorithm:-

a) Divide the large message into small number of blocks where each block represents the same range.
b) By raising the e^{th} power to module n encrypt the message.
c) For the decryption of message increase another power d module n.

2.7. Diffie- Hellman Key Exchange

Diffie Hellman key exchange algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. [7] Diffie Hellman also required two different keys. In Diffie Hellman Key Exchange, a shared secret key established, that is used that is used for communication over the public network. In Diffie Hellman Key Exchange Algorithm Sender and Receiver picks two secret numbers and these numbers are known to both sender and receiver. Let the number selected by sender is N_s and number selected by receiver is N_r then sender and receiver will generate a secrete key by calculating T_a.

$T_s = g^{sr} \bmod p$

Here, $g = |p|$

p is a large prime number

$g < p$

After calculating T_s and T_r, sender and receiver will exchange their values with each other, if they find that both the values are same, then communication starts.

3. Conclusion

Cloud computing appears very useful service for many people; every third person is using cloud in different ways. Due to its flexibility, many persons are transferring their data to cloud. Cloud computing prove a very successful application for organisations. Because organisations have large amount of data to store and cloud provides that space to its user and also allows its user to access their data from anywhere anytime easily.

As people are saving their personal and important data to clouds, so it becomes a major issue to store that data safely.

Many algorithms exist for the data security like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange and Homomorphic equations are asymmetric, in which two different keys are used for encryption and decryption. These algorithms are not secure, there is need to enhance the security of algorithms.

4. Future Scope

Cloud computing opens several new trends, like using software that are not present on your computer, accessing data from anywhere. One of the big advantage of cloud computing is virtualization, but we can use cloud computing properly only if it provide reliable security. Cloud computing is mostly used because it provides much storage space to its user, so it becomes necessary to provide security to that data. There are many security algorithms, but security of all these algorithms can be broken by anyone. So it is very necessary to make security of cloud more strong.

References

[1] Jawahar Thakur and Nagesh Kumar, 'DES, AES, Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis', International Journal of Emerging Technologies and Advanced Engineering (IJETAE). December **(2011)**, ISSN: 2250-2459 Vol. 1, Issue 2.

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

[3] Rachna Jain and Ankur Aggarwal 'Cloud Computing Security Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. January **(2014)** Vol. 4, Issue 1.

[4] Pratap Chandra Mandal, 'Superiority of Blowfish Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. September **(2012)** ISSN: 2277-128X Vol. 2, Issue 7.

[5] Sandipan Basu, 'International Data Encryption Algorithm (IDEA) - A Typical Illustration', Journal of Global Research in Computer Science. July **(2011)** ISSN: 2229-371X Vol. 2, Issue 7.

[6] B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, 'A Modified RSA Cryptosystem Based on 'n' Prime Number', International Journal of Engineering and Computer Science. Nov **(2012)** ISSN: 2319-7242 Volume 1 Issue 2.
[7] Ayan Mahalanobis, 'Diffie-Hellman Key Exchange Protocol', Its Gernalization and Nilpotent Groups. August **(2005)**.
[8] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. **(2011)**.
[9] Shakeeba S. Khan and Prof. R.R. Tuteja, 'Security in Cloud Computin Using Cryptographic Algorithms', International Journal of Innovative Research in Computer and Communication Engineering. January 1, **(2015)** ISSN (online): 2320-9801, (Print): 2320-9798 Vol. 3, Issue.
[10] Maha TEBAA, Said EL HAJJI and Abdellatif EL GHAJI, 'Homomorphic Encryption Applied to the Cloud Computing Security', World Congress on Engineering. July 4 **(2012)** Vol. 1, London U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (online).
[11] G. Devi and 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. **(2012)** Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596.
[12] Manzoor Hussain Dar, Pardeep Mittal and Vinod Kumar, 'A Comparative Study of Cryptographic Algorithms', International Journal of Computer Science and Network. June **(2014)** ISSN(Online): 2277-5420, Volume 3, Issue 3.
[13] Rashmi Nigoti, Manoj Jhuria and Dr. Shailendra Singh, 'A survey of Cryptographic Algorithm for Cloud Computing', International Journal of Emerging Technologies in Computational and Applied Science.**(2013)** ISSN(Print): 2279-0047, (Online): 2279-0055.
[14] Mohit Marwaha, Rajeev Bedi, Amritpal Singh and Tejinder Singh, 'Comparative Analysis of Cryptographic Algorithms', International Journal of Advanced Engineering Technology. July-Sept. **(2013)** E-ISSN 0976-3945.
[15] Simar Preet Singh and Gurpinder Singh Samra, 'Managing Vulnerabilites in Cloud Computing', National Conference on Engineering Applications(NCEA-2011), St. Solider Institute of Emerging Technology and Management, Jalandhar, Punjab. April 9 **(2011)** pg 243-246.

Authors

Ashima Pansotra, she received the degree of B.Tech (Computer Science & Engineering) from Global Institute of Management and Emerging Technologies, Amritsar (India) in 2014 and persuing her M.Tech (Computer Science & Engineering) from DAV University, Jalandhar (India). She has knowledge of Andriod and Java. Being a keen interest towards research, her interest area includes Cloud Computing and Lane detection.

Simar Preet Singh, he received the degree of B.Tech (Computer Science & Engineering) from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (India) in 2009 and M.Tech (Computer Science & Engineering) from Punjabi University, Patiala (India), in 2011. He has worked in Infosys Limited for two years. He is a lifetime member of Anti-Hacking Anticipation Society, India. Apart from this, he is also having certifications like Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Technology Specialist (MCTS) and Core Java. He had undergone training programme for VB.Net and Cisco Certified Network Associates (CCNA). He has presented many research papers in various National and International Journals/Conferences in India and abroad. His area of interest includes Network Security and Cloud Computing. He is presently working as Assistant Professor in 'Computer Science & Engineering' at DAV University, Jalandhar (India).

