International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

An Advanced Security Analysis by Using Blowfish Algorithm

R. Vasantha[1], Dr. R. Satya Prasad[2]
[1]Research Scholar, Department of CSE, Acharya Nagarjuna University, Guntur, India
[2]Associate Professor, Department of CSE, Acharya Nagarjuna University, Guntur, India

ABSTRACT

Cloud computing give off an impression of being an extremely prominent and intriguing processing innovation. Each third individual is utilizing distributed computing straightforwardly or in a roundabout way for instance email, most usually utilized utilization of distributed computing, you can get to your mail anyplace whenever. Your email account isn't unmistakable on your PC yet you need to get to that with the assistance of web. Like email distributed computing give numerous different administrations, for example, stockpiling of any sort of information, access to various applications, assets and so forth. So clients can undoubtedly access and store information with ease and without stressing over how these administrations are given to client. Because of this adaptability everybody is exchanging information to cloud. To store information on cloud client needs to send their information to the outsider who will oversee and store information. So it is imperative for the organization to secure that information. Information is said to be secured if secrecy, accessibility, trustworthiness is available. To secure information we have distinctive calculations. In this paper we will talk about the diverse cryptography of algorithms.

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

I. INTRODUCTION

Cloud isjust the social affair of servers and datacenters that are put at better places and these isolates and datacenters are accountable for giving on ask for organization to its customers with help of web. The organization gave by cloud is truant on customer's PC. Customer needs to get to these organizations with help of web relationship through subscribing them. The central favored point of view of Cloud preparing is that it abstains from the necessity for customer to be in same zone where hardware programming and storage space is physically present. Cloud makes it possible to store and access your data from wherever at whatever point without obsessing about help of gear programming and storage space. Each one of these organizations are given to customer expecting next to zero exertion. Customer needs to pay according to storage space he is using. In light of this flexibility everyone is trading his data on cloud. Security ends up being gigantic issue when any one stores its basic information to a phase which isn't particularly controlled by the customer and which is far away [8]. While sending of data and in the midst of limit data is under threat in light of the way that any unapproved customer can get to it, change it, so there is need to secure data. A data is secure, on the off chance that it satisfies three conditions

(1) Confidentiality
(2) Integrity
(3) Availability

Confidentiality implies the information is justifiable to the collector just for all others it would be squander; it helps in keeping the unapproved exposure of touchy data. Respectability implies information got by collector ought to be in a similar frame, the sender sends it; trustworthiness helps in keeping adjustment from unapproved client. Accessibility alludes to confirmation that client approaches data whenever and to any system. In the cloud classification is gotten by cryptography.

Cryptography is a technique of changing over data into befuddled edge in the midst of limit and transmission

that it appears to be waste to interloper. The limitless sort of data is known as figure content. Right when data is gotten by recipient it, will appear in its one of a kind casing which is known as plain substance. Change of plain substance to figure content is known as encryption and modify of this (figure substance to plain) is known as unscrambling. Encryption occurs at sender's end however unscrambling occurs at beneficiary's end.

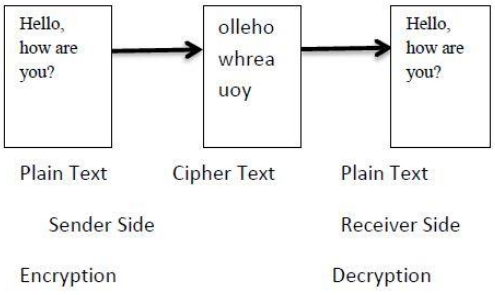

Figure 1. Encryption Decryption Process

There are three types of cryptography algorithms

(1) Symmetric algorithms
(2)Asymmetric algorithms
(3) Hashing.

In hashing a settled length mark is made with the assistance of calculations or hash work for the encryption of information. Each message comprises of various hash esteem, yet the hashing has one downside i.e. once the information is scrambled, it can't be unscrambled. This confinement of hashing was evacuated by symmetric and awry calculations. Symmetric calculation is otherwise called "Mystery Key Encryption Algorithm" in symmetric key calculation, just a single key is utilized for encryption and unscrambling i.e. private key, where as in hilter kilter calculation both open and private keys are utilized for encryption and decoding, uneven calculation is otherwise called "Open Key Encryption Algorithm"[1].

II. 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 commonly utilized symmetric key estimation. It was made by IBM in 1974, yet now a days various systems are found that had exhibited this count unsecured [1]. In DES counts square figure 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 piece figure we encode square of data which include plain substance by blend of confuse and scattering to impact figure to piece then this figure piece needs to pass 16 rounds, before experiencing these 16 changes the 64 bits of data is parceled into 32 bits. In the wake of confining the data into 32 bits, F-work (Feistel work) is associated. F-work includes substitution, arrange, key mixing. The yield of limit is joined with other segment of the data using XOR portal trade crossing point of data is done; by then convergence of data is done.

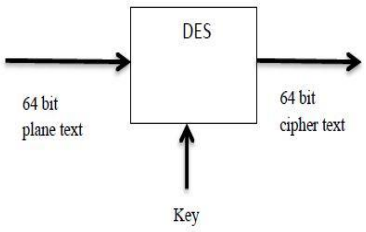

Figure 2. High Level Diagram of DES Encryption Algorithm

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 Lf and Rf than F function and XOR operation is applied on Rf, and output is combined with Lf.

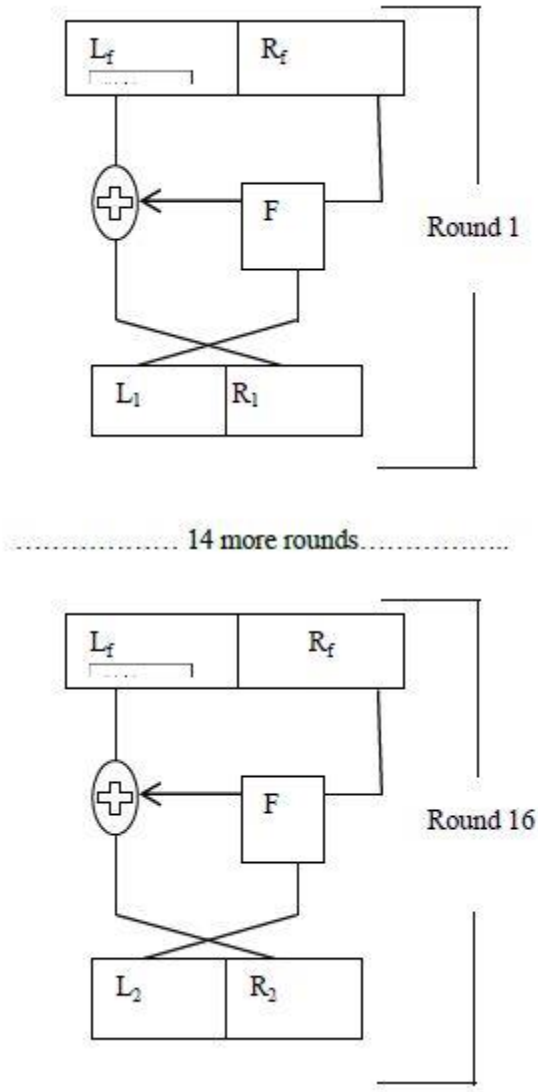

Figure 3. Inside Working of DES Algorithm

2.2. Advance Encryption Algorithm (AES)

AdvanceEncryption calculation AES is otherwise called Rijndael. AES is declared as U.S FIPS by NIST in 2001. In AES, diverse size of key is utilized i.e. 128, 192 or 256 bdepends on what number of cycle it utilizes [3]. For 10 cycles 128-piece key, 12 cycles 192 piece key and for 14 cycles 256 piece key is utilized. All rounds of AES are comparable aside from the last one. AES takes a shot at 4x4 frameworks. AES comprises of key extension, beginning and last round. Beginning round comprise of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and last round likewise comprises of comparable capacity as starting round with the exception of blend sections. AES works quick on both programming and equipment.

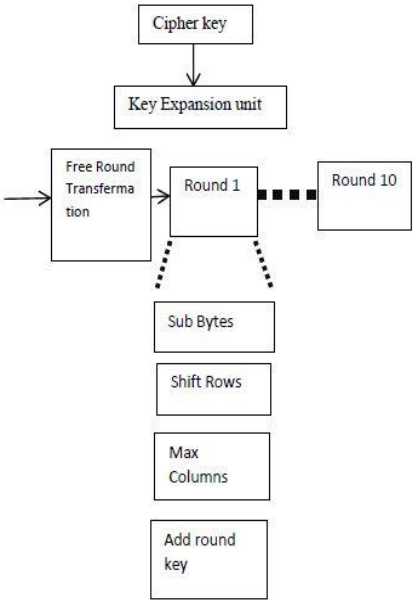

Figure 4. Encryption with AES Algorithm [13]

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.

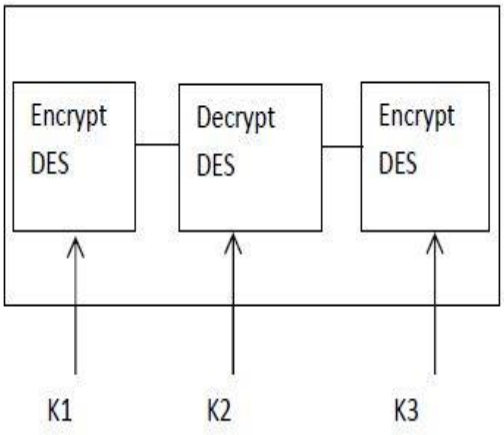

Figure 5. TDES Encryption Algorithm [13]

2.4. Blowfish Algorithm

Blowfish Algorithm is a symmetric key calculation which was created in 1993 by Bruce Schneier. Its working is practically like DES yet in DES key size is little and can be unscrambled effectively yet in Blowfish calculation the measure of key is substantial [4] and it can shift from 32 to 448 bits. Blowfish

likewise comprises of 16 rounds like DES [11]. Blowfish figuring can scramble data having size different of eight and if the measure of the message isn't diverse of eight than bits are padded. In Blowfish computation in like manner 64 bits of plain substance is parceled into two areas of size 32 bits. One area taken as the left bit of message and other is right bit of message. The left part is XOR with the segments of P-group which makes some regard, by then that regard is experienced change work F. The regard began from the change work is again XOR with the other bit of the message i.e. with right bits, by then F| work is called which supplant the left half of the message and P| supplant the right side message.

2.4. Thought

Worldwide Information Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key figuring. It perceives 64 bits plain substance and key size is 128 bits. Thought incorporates 8.5 rounds. Despite rounds are relative from the one. In IDEA the 64 bits of information is isolates into 4 hinders each having size 16 bits. Before long key operations measured, expansion, duplication, and bitwise specific OR (XOR) are related on sub squares. There are eight and half changes in IDEA each round contain diverse sub keys. Demonstrate number of keys utilized for performing different rounds is 52. In cycle 1 the K1 to K6 sub keys are made, the sub key K1 has the hidden 16 bits of the central key and K2 has the going with 16 bits also for K3, K4, K5 and K6. In this way for cycle 1 (16*6=96) 96 bits of exceptional figure key is used. What is the gathering of operations performed in each round? Let I1, I2 … I6 be the commitments to [5]
cycle 1, works in round 1 are:-

(i) Multiply I1 and K1.
(ii) Add I2 and K2.
(iii) Add I3 and K3.
(iv) Multiply I4 and K4.
(v) Now, step 1 is EXOR with step 3.
(vi) Step 2 EXOR with step 4.
(vii) Multiply step 5 with K5.

Similar operations are performed in other rounds.

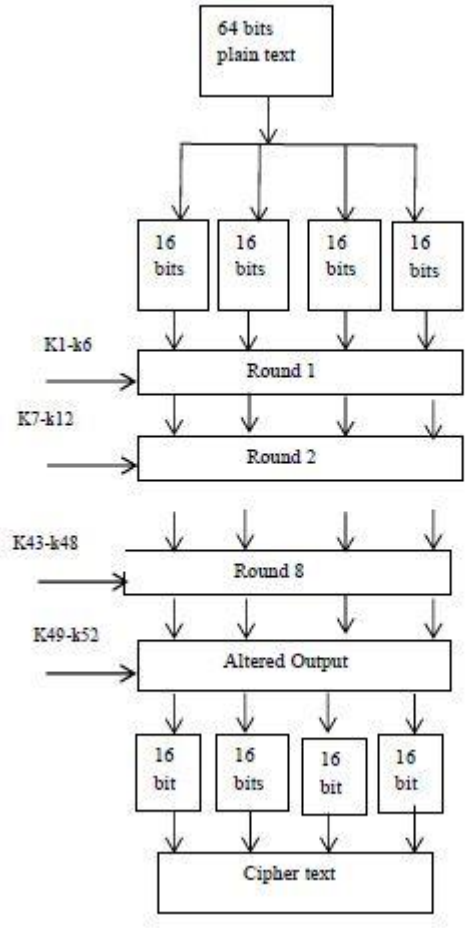

Figure 6. Encryption with IDEA

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 eth 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 Ns and number selected by receiver is Nr then sender and receiver will generate a secrete key by calculating Ta.

Ts= gsr mod p

Here, g =|p|

p is a large prime number

g < p

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

III. CONCLUSION

Cloud enrolling appears to be to a great degree accommodating organization for a few people; every third individual is using cloud in different ways. As a result of its versatility, various individuals are trading their data to cloud. Disseminated registering exhibit a greatly viable application for affiliations. Since affiliations have broad measure of data to store and cloud gives that space to its customer and moreover empowers its customer to get to their data from wherever at whatever point easily. As people are saving their own and basic data to fogs, so it transforms into a vital issue to store that datasecurely.

Numerous calculations exist for the information security like DES, AES, and Triple DES. These are symmetric key calculations in which a solitary key is utilized for encryption and decoding though 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.

IV. Future Scope

Cloud computing opens a few new patterns, such as utilizing programming that are absent on your PC, getting to information from anyplace. One of the enormous preferred stand point of distributed computing is virtualization, yet we can utilize distributed computing appropriately just in the event that it give dependable security. Distributed computing is generally utilized on the grounds that it gives much storage room to its client, so it ends up noticeably important to give security to that information. There are numerous security calculations, however security of every one of these calculations can be broken by anyone. So it is very necessary to make security of cloud more strong.

V. REFERENCES

[1]. Alexa Huth and James Cebula ‘The Basics of IOT, United States Computer Emergency Readiness Team. (2011).

[2]. Anitha Y, "Security Issues in cloud computing with IOT", "International Journal of Thesis Projects and Dissertations "(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.

[3]. Qi. Zhang Lu. Cheng, Raouf Boutaba, "Cloud computing IOT : state-Of-the-art and research Challenges", "The Brazilian Computer Society", April 2010.

[4]. Garima Saini, Gurgaon Naveen Sharma,"Triple Security of Data in Cloud Computing IOT ", Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4) , 2014,

[5]. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[6]. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
[7]. Gurpreet Singh, Supriya Kinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security IOT" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2016.
[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.