ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Implementation of Encryption Algorithm for Data Security in Cloud Computing

Khasim Shaik
Asst. Professor, Department of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

N.Sharath kumar
Student, Department of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Thota Venkat Narayana Rao
Professor, Department of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Abstract: Cloud computing is the present technology which is gaining greater attentions. Nowadays, among all the technologies that includes the network security, data protections, virtualization security, application integrity and identity management, the cloud is the most essential and key aspect. Among all the above mentioned issues, data protection is one of the most important security element because organizations cannot transfer their data to the remote machines as there is no guarantee of data protection by the cloud service providers. Many techniques are already available to protect the data in cloud. Though there are many number of techniques implemented to have focus on security of data but still some challenges persist. Cloud computing solves not only the computing problems but also caters loads of data with software updates etc. The user will be confident in utilising the cloud sources only if there is an appropriate collaboration between cloud client and cloud service provider. The most popular security techniques include SSL (Secure Socket Layer) Encryption, Algorithms like AES, Blowfish, DES, RSA, Cloud Computing, and Data Security. This paper mainly focus on how to analyse and evaluate the most important security encryption algorithms for data protection in cloud computing. Furthermore, this paper also discusses about some of the new security techniques for data protection which will be recommended in order to have improved security in cloud computing.

Keywords: Cloud, Data Protection, Security, Asymmetric Algorithms, Symmetric Algorithm.

I. INTRODUCTION

Before we discuss about cloud computing and its challenges towards the data protection, we must first understand the concept of cryptography [2]. Cryptography is the heart of both data security and communication media. It is a popular technique in the software organizations until recently and every citizen from developed countries uses it daily for their business needs. It is used for providing authentication and encryption of data. This technique is mostly used in e-commerce transactions and access control (car lock systems, ski lifts), payment (prepaid telephone cards, e-cash), and has become the most fundamental instrument of democracy with the e-voting systems. The master cryptographic tools have become a greater requirement for most of the engineers. Cryptographic Algorithms plays a major role in an implementation of encryption of data for data security. As the complexity of algorithm is high, the risk of breaking the original plain text from that of cipher text is less. Greater complexity in the algorithm makes its security greater[5][3].

The cryptographic algorithms are majorly categorized into symmetric and asymmetric key cryptography. Symmetric key encryption algorithm uses a usual key for both encryption and decryption of data. As we know a key always plays an important role in both encryption and decryption. If a key used in the algorithm is uncertain, then it can be easily decrypt the data which can be seen by the attacker. The maximum possible length for key size determines the strength of the symmetric key encryption. The symmetric algorithms are generally of two types. They are stream ciphers and block ciphers. Stream cipher will be operated on data. Every plain text digit is encrypted one at a time with corresponding digit of the key stream. The block ciphers are operated on data in groups or blocks. Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish which are solely based upon block cipher and moreover they are the algorithms of symmetric key encryption. In asymmetric key encryption or public key encryption it uses two keys, one is private key which is used for decryption of data and other is public key which is used for encryption of data. As shown below, fig 1.1 shows the overview of field of cryptography[4][8].

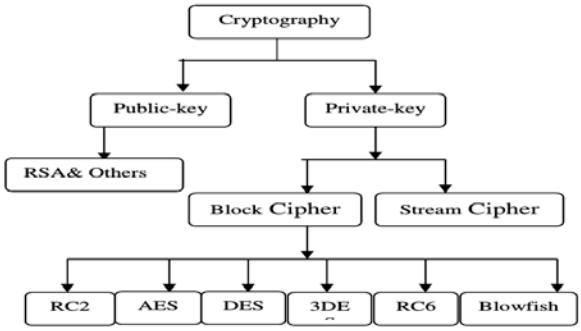

Fig 1.1: Overview of field of cryptography

1.1 Research motivation and objectives

Cloud computing user's work with data based on applications which are often located off-premise and stored in remote areas[8]. However, many organizations are

uncomfortable with the idea of having their data and applications on systems that they do not control.

They are unaware of how cloud computing impacts [9] the confidentiality, integrity of data stored, processed and transmitted in cloud computing environments [6]. The major goal of this paper is to create a framework that clarifies the impact of cloud computing on confidentiality preservation, by making stepwise recommendations on:

- How data can be classified on confidentiality?
- How data classifications relate to the security controls needed to preserve the confidentiality of data?
- How the process of security control selection is negatively influenced in cloud computing environments?
- How to cope up with the negative influences of cloud computing on the protection of data confidentiality?

II. BACKGROUND STUDY

Cloud computing is basically broken down into three segments: "application", "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses around the world. The services of cloud have long been referred to as Software as a Service (SaaS). There is an increasingly perceived vision that the computing will become the 5th utility (after water, electricity, gas, and telephony). This will become one of the basic utility. To deliver this vision, architecture was made for creating cloud. Cloud computing is the concept which is implemented to decipher daily computing problems, like the Hardware, Software and Resource Availability, unhurried by Computer users. The cloud computing provides an undemanding and non ineffectual solution for daily computing. The frequently occurred problem associated with cloud computing is the cloud security and the appropriate implementation of cloud over the network. With the help of different encryption algorithms like DES, AES and BLOWFISH the users can be able to enhance the data security of cloud computing[5][7].

III. OBJECTIVE OF THE WORK

The objectives of the proposed work are given below. They are:

- To create a secure cloud architecture.
- Cloud access control and management of key.
- Privacy identification in cloud.
- Protection of remote data.
- Secure operation for dynamic data.
- Security to both software and data segregation.
- Secured management of virtualized resource.
- Protocol design for both joint security and privacy aware protocol.
- Prediction of failure detection.
- Availability, recovery and auditing.
- To provide a secured wireless cloud.

IV. PROPOSED STEPS OF THE WORK

In this paper different encryption algorithms like AES, DES, RSA and Blowfish to ensure the security of data in cloud are used. For the perspective of different users, these algorithms are proposed and used in many aspects. The algorithm DES is developed in early 1970's and Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001. All of these algorithms are symmetric key, in which a single key is used for encryption and decryption of data. RSA is Asymmetric key algorithm which was developed by Ron Rivest, Adi Shamir and Lenard Adleman in early 1978. This algorithm is majorly used for public key cryptography. In this, two keys are used, one is public key which is used for encryption and other is private key which is used for decryption of data. In this there can be an option to the users to choose any algorithm according to their convenience and then encrypt/decrypt the data on cloud respectively. Here the Java runtime environment of Google App Engine, i.e. JDK 1.6. Eclipse IDE, Google App Engine SDK 1.6.0 or higher are used to have experimental setup. Google Plug-in for Eclipse, for creating, debugging and testing the application are all provided in the environment. Below fig-4.1 shows the steps which are related to the proposed work.

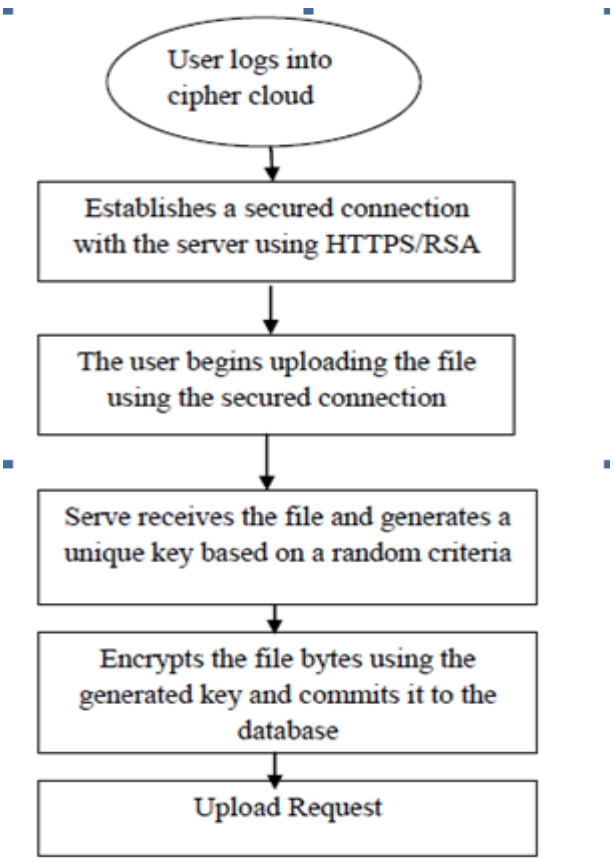

Fig 4.1: Proposed Steps of the work

V. GOALS OF THE RELATED WORK

In order to provide a better system to maintain security to the data few parameters which are to be considered they are:

1) Confidentiality: It focus on the information which is in computer has to be only accessed by the authorized party but not by anyone else.
2) Authentication: The information or data which is received by any system has to check the sender identity and make sure that the information is arriving from an authorized person without any false identity.
3) Integrity: It pertains only the authorized party can be allowed to modify the data or information. No one, in between the sender and receiver are allowed to make changes for given message.
4) Non Repudiation: It ensures that neither the message sender, nor the message receiver should be able to deny the transmission of appropriate message.
5) Access control: Only the authorized parties can be able to access the provided information.

VI. TERMINOLOGY RELATED TO THE WORK

To understand more about the paper below we given some basic terminology related to the technology. They are:

1) Plain Text: If a person wants to communicate with other person the original message which was sent by sender called as Plain Text. For example, Alice is a person who wishes to send "Hello Friend, how are you?" message to the person Bob. Here "Hello Friend, how are you?" is a plain text message.

2) Cipher Text: The message which cannot be understood and read by any one or a message which doesn't have appropriated meaning, we call it as a cipher text. For Example, "Ajd672#@91ukl8*^5%" is a Cipher Text which is produced for "Hello Friend, how are you?"

3) Encryption: The technique of converting a plain text into cipher text is defines as Encryption. The encryption technique has to consider two basic things- at first an encryption algorithm and second a key. An encryption algorithm means the technique that has been used in encryption. This entire technique which takes place at the sender side alone.

4) Decryption: The reverse process of previously mentioned i.e. encryption technique can be called as Decryption. It is basically a process in which the conversion of cipher text into equivalent plain text or unreadable text into the readable text. Again the process of decryption requires two major things- first a decryption algorithm second a key. A decryption algorithm means the technique which has been used in Decryption. Basically both the encryption and decryption algorithms are same and the key is same for encryption and decryption.

5) Key: Generally a key is either a numeric or alpha numeric text or may be some special symbol. The key can be used during the time of encryption on the plain text and also during the time of decryption which takes place on the cipher text. For example, if the Alice uses a key of three to encrypt the plain text "President" then cipher text produced will be "Suhylghqw".

VII. DEALING CRYPTOGRAPHIC ALGORITHMS

There are many cryptographic algorithms that are available to be used for both encryption and decryption of data and majorly, they fall into two generic categories. One is of public key system and other deals with secret key system. Symmetric key algorithm is called as secrecy key or shared key algorithm, because in symmetric key algorithm a shared key can perform both the encryption and decryption of data. Only one key is used for doing everything, so the success ratio of the algorithm depends upon two bright factors which are secrecy of the key and its distribution. The symmetric algorithms are: Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption algorithm (IDEA), Blowfish, Advanced Encryption Standard (AES). Asymmetric key algorithm is called as public key algorithm. In this algorithm, there are two keys, one is public key and other is private key which are used for both encryption and decryption of data. Public key is used to encrypt the message and private key is used to decrypt the message. Asymmetric algorithms are Diffe-Hellman and RSA Public Key Encryption. Symmetric key technique works with the help of a single key called secret key which uses limited mathematics, results into the lower computation, on the other hand asymmetric key technique takes the help of both public key and private keys, which results in good amount of processing and occupies added energy and heavier secure. Symmetric key techniques provides superior energy efficiency in comparison to public key due to this is most of the researches make it use of it in their work in order to create MAC in WSN.

A. AES

The NIST (National institute of standards and technology) chosen the Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen, to replace the data encryption standard (DES) algorithm as the modern advanced encryption standard (AES) algorithm. AES algorithm is based on a design principle which is called as a substitution-permutation network. This algorithm has 128-bit block size and a key size permitted to either 128,192 or 256 bits. AES accomplish on a 44 column-major order matrix of bytes, termed the state of algorithm. Majority of AES computations are done in a particular finite field. The AES cipher is noted as a number of repetitions of transformation of rounds which converts the plain text input into the text output which cannot be able to read by a human. The number of cycles of repetition is as follows:

a. 10 cycles of repetition for 128 bit keys.
b. 12 cycles of repetition for 192 bit keys.
c. 14 cycles of repetition for 256 bit keys.

For the encryption process some of the operations are required they are as follows: SubBytes, ShiftRows, MixColumns and XorRoundkey. And for the Decryption is the exact reverse process of encryption which mainly uses

inverse functions: InvSubBytes, InvShiftRows and InvMixColumns. An easiest way to view the AES order of function is: 16

1. Scramble each byte (SubBytes).
2. Mix up each row bits (ShiftRows).
3. Scramble each column bits (MixColumns).
4. Encrypt (AddRoundKey).

B. Blowfish

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm works with two parts: a key expansion part and a data encryption part. The key role of key expansion part is to convert a key of utmost 448 bits into several keys of sub arrays with the sum as 4168 bytes. The data encryption occurs via a 16-round Feiste- network. It is only suitable for application where there is no change in key, often like communications link or an automatic file encryption. It is considerably faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. The nature of encryption algorithms is that, once any significant amount of security analysis is done, it is undesirable to vary the algorithm for performance reasons, there by invalidating the results of the analysis. Thus, it is necessary to consider both data security and performance together during the design phase. While it is impossible to take all future computer architectures into consideration, an understanding of common optimization guidelines, combined with exploratory software implementation on existing architectures to standardize performance, which aids in achieving higher speed in prospective encryption algorithms.

C. Subkeys

The Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption. The P-array consists of 18, 32-bit subkeys: P1, P2... P18. There are four 32-bit S-boxes with 256 entries each: S1,0, S1,1,..., S1,255; S2,0, S2,1,..,, S2,255; S3,0, S3,1,..., S3,255; S4,0, S4,1,..,, S4,255.

D. Pseudo Code of Blowfish Algorithm

At initiation the Blowfish algorithm has 16 rounds. The input is of 64-bit data element, x. Divide x into two 32-bit halves: xL, xR. xL is the left side half and xR is the right side half. Then, for i = 1 to 16, the rounds should be implemented: xL = xL XOR Pi xR = F (xL) XOR xR. Swap xL and xR after the sixteenth round and then swap xL and xR again to undo the last swap. Then, xR = xR XOR P17 and xL = xL XOR P18. Finally, recombine xL and xR to get the cipher text, which is not logical. Decryption process is exactly identical as encryption, except that P1, P2 and so on unto P18 which are used in the reverse order. Implementations of Blowfish also requires the fastest speed to unroll the loop and ensures that all subkeys are stored in cache[10].

VIII. COMPARISION OF ALGORITHMS WITH SIMULATION RESULTS

The calculation for decryption and Encryption speed for each algorithm with different packet sizes has been tested. The implementation tried to optimize the maximum performance for the algorithm. The throughput for decryption as well as encryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption scheme. The performance metrics are analyzed in Matlab upon consideration of two basic parameters which are (a) Time for encryption and decryption, (b) Time taken by CPU processor which is as shown in below tables 8.1 and 8.2 including a simple chart representation shown in fig 8.3.

Table -8.1: Comparison of algorithms with respect to block size.

Algorithm	Block Size	Rounds	Key
AES	128,192,256 Bits	10,12,14 Rounds	128 Bits
BLOWFISH	32-448 Bits	16 Rounds	64 Bits

Table 8.2: Comparison of algorithms w.r.t time in seconds

algorithm	Encryption/decryption For 64 bits	CPU Time
AES	1.261816	1.54440990
BLOWFISH	0.850568721	0.07800050

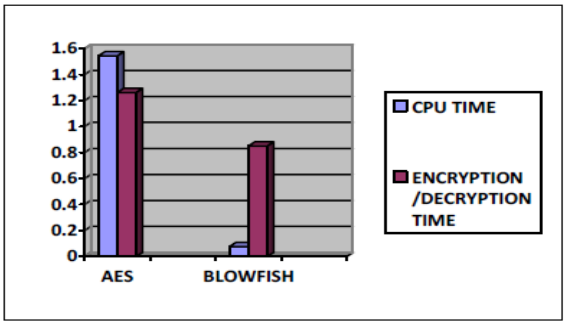

Fig 8.3: comparision of algorithms in a bar-chart represenation

IX. CONCLUSION

The simulation which was depicted in this paper shows the influence that, the Blowfish encryption algorithm with coordination to the AES encryption algorithm upon consideration of two major parameters throughput and processing time. Whenever higher throughput exist, the

speed becomes high, whenever the above situation arises it is also observed that the power consumption is less. Finally it is concluded that the Blowfish is the optimized one among all available algorithms. In future scope of the proposed paper, one can also add hardware implementation as a parameter and proceed to its implementation to compare different parameters.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[3] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[4] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[5] Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, pp. 1328-1334, 2010

[6] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[7] Ronald L. Krutz, Russerll Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010

[8] X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", In Proceedings of 10th IEEE International Conference on Computer and InformationTechnology.

[9] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[10] Chaitali Haldankar, Sonia Kuwelkar, Implementation Of Aes And Blowfish Algorithm, International Journal of Research in Engineering and Technology, Volume: 03 , Issue: 03 | May 2014.