A survey on Cryptography Algorithms in Cloud Computing Environments

Nasreen Ahmed Mekki, Omer A. Sharif, and Amin B. A. Alnabi

Al Neelain University

GCNU Journal

ISSN: 1858-6228

Volume 16 - 2021
Issue: 03

Graduate College

Al Neelain University

Graduate College Journal – NU
Vol.16 -2020, No. (3)
ISSN: 1858-6228, http://www.neelain .edu.sd

مجلة الدراسات العليا - جامعة النيلين
المجلد (16) –2020، العدد (3)
الرقم الدولي الموحد للدوريات: 1858-6228

A survey on Cryptography Algorithms in Cloud Computing Environments

Nasreen Ahmed Mekki, Omer A. Sharif, and Amin B. A. Alnabi

[1]Faculty of Engineering, Sudan University of Science and Technology, Khartoum, Sudan.
[2]Algareen Engineering. "Innovation for the Nation", Khartoum, Sudan.
Faculty of Engineering, Al Neelain University, Khartoum, Sudan
Corresponding author E-mail: Nasreenmekki@yahoo.com

Abstract

Cloud computing is a big platform in the field of information technology for sharing data, resources, services and information by people of the world. The big problem in cloud is security, there are many method used to create secured data in cloud computing. Cryptography is one of an effective method to create secure communication in cloud computing especially in real time application where either symmetric key or a symmetric key can be applied. This paper presents a survey of many papers, which uses many encryption algorithms, many of them uses symmetric algorithms, the others papers uses asymmetric algorithm, and the others papers uses symmetric and asymmetric algorithms. The objective of this paper is to select or achieve suitable algorithm for their suitable application to encrypt data in a secure manner. The important goal of all papers in this survey is encryption time, decryption time, and throughput. In this paper a comprehensive survey has been done on the encryption algorithms in different applications that are similar to the applications in the cloud computing environment to select a suitable encryption algorithm to encrypt storage data in a secure manner

Keywords: Cryptography, Encryption, Decryption.

Introduction

Cloud computing is the technology, which shared resources and software information to the world, this technology supports distributed data processing, which provides service to multiple external customers through the world wide web, cloud service providers provide many applications for the cloud to be secure (Nafi et al., 2013). To protect sensitive data from unauthorized uses there are many methods, cryptography is one of an effective method to create secure communication in cloud environment**,** such that only the receiver can be able to retrieve the sent information to provide message confidentiality, data integrity, authentication, non-repudiation, and encryption and decryption process. Cryptography is a science of using mathematics to encrypt and decrypt sensitive data to store it in a secure manner, when you want to store that sensitive data or transmit it over network to protect it from attacks.

A cryptosystem consists of cryptography algorithm, that describe by a mathematical function to encrypt input message with their input key to find a cipher message or decrypt the output of the cipher message to return the input message to it is original form. Cryptography algorithms are divided into two categories: symmetric algorithm, and asymmetric algorithm. Symmetric algorithms are those algorithms in which sender and receiver use same key for encryption and decryption process. But asymmetric algorithms are those algorithms which sender and receiver have different keys for encryption and decryption process (Sharma (2017).

The important parameters in the selected encryption algorithm are the computability, simplicity, complexity of encryption algorithm, the encryption execution time, and the through put.

Data Encryption Standard Algorithm (DES)

Data encryption standard published in 1997 by National Bureu of standard, the algorithm has two inputs to be encrypted plain text of 64 bits, and the key of 64 bits, it transforms these two inputs in a series of steps start from initial permutation to rearrange the plain text new order, then divide it into two part right half, and left half of 32 bits to generate 16 round function of the same function. This round function has permutation, and substitution function to find the pre-output, and then the pre-output passed through the inverse permutation (IP^{-1}) to find the 64 bits cipher text (Sir, 2017).

Blow fish algorithm

Blow fish is a symmetric cipher developed by Bruce Schneider is designed to be fast, compact, simple, and very secure. The key length of the algorithm is 48 bits long the structure of the algorithm. The algorithm encrypts 64 bits blocks of plaintext into 64 bits blocks cipher text. Blow fish operate on both halves of the data in each round, this algorithm provide greater cryptography when we compare it by classic Feistel cipher (Sir, 2017).

Advanced Encryption Standard Algorithm (AES)

Advanced Encryption Standard (AES) published by the National Institute of Standard Technology (NIST) in 2001, this standard specifies the Rijndael algorithm is a symmetric block cipher of data blocks of 128 bits using the different keys lengths of 128, 192, 256 bits. The encryption processes consists of N rounds, the number of round depends on the key length, 16 bytes key has 10 rounds, 24 bytes key has 12 rounds, and 32 bytes key has 14 rounds. Each round consists of four transformation function: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The final round contains only three transformations, and there is an initial transformation (AddRoundKey) before the first round. Each transformation takes one or more 4×4 matrices as input and produces output of 4×4matrix (Stallings, 2011).

Rivest-Shamir-Adleman (RSA)

RSA is asymmetric encryption algorithm block cipher, the plain text and cipher text of this algorithm is an integers between 0 and n-1 for n number, where n is less than 2^{1024}, the block size must be less or equal to $\log_2(n)+1$, the block size is i bits, where $2^i < n \leq 2^{i+1}$

For encryption process the cipher text block C is: $= M^e mod\ n$, and for the decryption process the plain text block M is: $M = C^d mod\ n$, the sender knows the value of e, then it has public key PU = {e,n}, and the receiver only knows the value of d, then it has private key PR = {d,n} (Stallings, 2011).

RC4

RC4 is a stream cipher, it has two working modules, the first is the key k input (size of 256 bits), and the second is PRGA which generates pseudo- random output sequence. The RC4 encryption algorithm is to generate 256 bytes initial state vectors with a random key k. The expanded key is generated a secret key k is of length l bytes, the expanded key will be:

$k[i] = k[imodl] for\ 0 \leq i \leq N-1$, when the output of the expanded key is achieved, then XORed to the second module PRGA of plaintext to produce a cipher text (Rajoriya and Mohota, 2017)

Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard is a developer of DES cryptographic algorithm using three key combinations for encryption and decryption process, the effective length of key is 168 bits consisting of three sub-keys each have length of 56 bits (Ratnadewi et al., 2018).

Literature Survey

Symmetric Encryption Algorithms

Many symmetric encryption algorithms are based on two cipher, stream ciphers and block ciphers; Stream cipher is encrypts a digital data stream one bit or one byte at a time like Vernam cipher or Vigenere cipher, and block ciphers is a digital data treated as a whole block which used to produced cipher text block of equal length like DES, AES, 3DES, RC4 algorithms (Stallings, 2011).

This section discusses the result of many papers related to symmetric encryption algorithm.

Muhammad Khan, proposed a new Fast-DES algorithm, which works in three rounds of block of 32 bits plaintext with key size of 32 bits to produced 32 bits encryption cipher text, this algorithm was design for high speed and provide good security in fast time (Khan et al., 2012).

Parkash, proposed an efficient data encryption to encrypt sensitive data before sending to cloud server. The proposed method reduced storage and computing over head by splitting of file and reduced the burden of data owner by access the data from the cloud server when an authorized user are verify. The experimental results show that the execution time is increase when the file size is increase. The disadvantage of the algorithm of the proposed method decryption time is taking more time than encryption time (Prakash et al., 2014)G L, et al, 2014).

Sivasankari et al design a proposed True Random Number Generation (TRNG) depends on examining two oscillators' frequencies utilizing Data flip flop using AES algorithm. The encryption and decryption engine require 128 bits for mystery key. The itemized structures or each of changes in AES calculation are increment speed every change is upgraded for execution. The encryption and decryption throughput of 38.65 Gbps at 175.452MHz and it is strong to physical attacks (Sivasankari et al., 2017).

Janapriya et al proposed system used a powerful two class SVM classifier to discriminate encrypted and non-encrypted image patches enabling us to decode embedded message and the original image signal perfectly, the system takes the original video, then convert it into number of frames or image then select the particular frame and add password graphically for more security and convert it into binary form, then apply AES technique, these replace by the binary data, then get a stego video and apply combined DCT technique to encrypt the data. The proposed system is more bit per pixel ratio, high compression ratio and complex free computation (Janapriya, 2017).

Ratnadewi1 et al proposed an application of data writing and data reading of ACOS3 smart card using DES and 3DES algorithm in NFC based system. The result of this examination is that DES encryption method for writing is faster than using 3DES encryption method for each observation data. The data reading process decryption method is faster than using 3DES encryption method for each observational data. The writing execution time of ACOS3 smart card using DES and 3DES decryption process is faster than encryption process for each observational data (Ratnadewi et al., 2018).

Ankit Shukla et al develop an application which allows the user to encrypt the message before transmitted over the network using AES algorithm to provide stronger security for communication network by enhancing AES algorithm to operates on 16×32 array of bytes, the input key for encryption is 512 bits. By using this algorithm sending and receiving mail is done without disturbing any third party and important message are store securely and remain undisclosed even when the device is accessed by an adversary (Ankit Shukla, 2018).

Amab et al proposed Modified Advanced Encryption Standard a light weight version of AES, which presented a new one dimensional substitution box is proposed by formulating a novel equation for constructing a square matrix of affine transformation, This algorithm has more energy efficiency, less number of packets at the same voltage degradation about 18.35%, and less average transmission time than the original Advanced Encryption Standard (AES), but the algorithm can't use other multimedia data (Nafi et al., 2013).

Asymmetric Encryption Algorithms

In this section asymmetric encryption algorithm paper are discuss to show the results and analyze it.

Faraz et al discussed six different asymmetric key of RSA, E-RSA algorithm is used as a proposed method because it is more secure against possible attacks in limited power device, but the total execution time for RSA is less than E-RSA. The disadvantage of this paper the author proposed two separate cloud server one for data and the other for key cloud, which create more storage and computation overhead (Moghaddam et al., 2013).

Cryptography Algorithms

Many papers proposed symmetric encryption algorithm only, others papers proposed asymmetric encryption algorithm only, and others papers proposed both symmetric and asymmetric encryption algorithms in their work.

Kawser et al proposed secure communication system and hiding information from others use AES for secured file encryption using 128 bits key, which is kept in the data base table. The user account name is hashed using MD5 algorithm, but RSA algorithm is used for secure communication of a synchronous key system, which make the system fragile in run process. The model system is more secure but the implementation take more time because each algorithm is done in different servers (Nafi et al., 2013).

Vishwa et al developed a new cryptography algorithm based on block cipher and logical operation XOR and shifting operation and compared between the proposed algorithm and AES, DJSA algorithm. The proposed method is more secure, simple, and much smaller time for encryption and decryption. It is impossible to break it without knowing the exact key value, but the implementation process is done for text file only (Gupta et al., 2012).

Ranchna et al proposed algorithm that eliminates the need to share any password and lets user to open files stored in the cloud specifically to the first computer which store on it by using the identification of the computer over the network as the security key, which will be used to encrypt the data. By this algorithm the data can be accessed from either a secure or unsecured network because the user having key with them. Keys will be generated separately on each device on initial setup but this makes the data secured with hardware lock of physical need to synchronization of data (Jain, 2014).

Manikandasaran et al discussed the different types of attacks on cloud data outsider's attack that can be protected by authentication mechanism, and insider attacks that are difficult to identify. To address the insider attacks it must be developed a new technique. The author shows that symmetric encryption algorithm is suitable for cloud data storage, but asymmetric encryption is much slower. The disadvantage of this paper the author cannot develop technique to protect the insider attacks (Manikandasaran, 2016).

Teja et al proposed a system using RSA, and AES encryption algorithm using USB device with random generated passkeys, which are very complex combinations. The proposed frame work will recognize USB that contains the private-key utilized for records to be downloaded from the cloud. In case if the gadget USB not available, the user can not upload the data. If the user wants to download any file, they needs to request a particular file, request will pass to auditor to get a secret key to their mail. The file will be downloaded when the system verify the user secret key. These methods provide the security and protecting their information from others and download any file from any device when the system verifies the users (Teja et al., 2017).

Kumari et al performs a comparative analysis of three algorithm AES, DES, and Blow fish for video encryption and decryption time in two parameters like time and file size as a result Blow fish has least encryption time, and DES has maximum encryption time. But Blow fish and AES algorithms have better decryption time than DES algorithm. The author shows that Blow fish algorithm is better than AES, and DES algorithms for encryption and decryption time, But for the file size the time is increase when the size are increase for encryption and decryption process (Kumari et al., 2017).

Comparison Studies of Symmetric Algorithms

No	Methods	DES	3DES	AES	RC4	Blow fish
1	Developed by	National Bureu of standard in 1997	IBM in 1998	National Institute of Standard Technology (NIST) in 2001	R. Baldwin and R. Rivest in October 1996	Bruce Schneier in 1993.
2	Structure of algorithm	Fiestel Network	Fiestel Network	Substitution and Permutation Network	Fiestel Network	Fiestel Network
3	Key length	64 bits	168 bits (3 sub key)	128, 192, 256 bits	256 bits	32 up to 448 bits
4	Block size	64 bits	64 bits	128, 192, 256 bits	256 bits	64 bits
5	No. of Round	16 Rounds	16 Rounds	12, 14, 16 Rounds	1 |Round	16 Rounds
6	Efficiency	slow	slow in software	Efficient in both Hardware and Software	Very slow in software	Highly efficient Software
7	Advantage	Faster than 3DES	More secure than DES	High throughput, reduced computation over head	Simple encryption and decryption algorithm	Best encryption, decryption time
8	Disadvantage	It is broken using brute-force	It is very slow in hardware and software implementation	In counter mode is complex to implement in software taking both performance and security into considerations	Led to very in secure algorithm protocols	Key management becomes complicated, can't provide authentication, weakness of decryption process, and serially in throughput.

Future Strategies

This paper is extended to define a new Modified AES algorithm, the new algorithm will be define for multi-core processor which operates in parallel processor or parallel computing to achieve minimum encryption and decryption time, and speed up the device measurement and performance.

Conclusion

A survey has been shown that Advanced Encryption Standard is more efficient for hardware and software, high throughput, strong to physical attacks, low complexity architecture, low latency for large data, and very low RAM space. For this reasons Advanced Encryption Standard is more suitable encryption algorithm for storage data security on cloud computing.

References

ANKIT SHUKLA, A. M., ASHISH SINGH RAWAT 2018 Encrypted Email System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 3**,** 2456-3307.

GUPTA, V., SINGH, G. & GUPTA, R. 2012. Advance cryptography algorithm for improving data security. *International Journal of Advanced Research in Computer Science and Software Engineering,* 2.

JAIN, R. 2014. Ankur Aggarwal 'Cloud Computing Security Algorithm'. *International Journal of Advanced Research in Computer Science and Software Engineering,* 4.

JANAPRIYA, B. 2017. Video Steganography Schema based on AES Algorithm and 2D Compressive Sensing. *Image,* 3**,** 4.

KHAN, M. N., WAHID, I. & IKRAM, A. A. 2012. The FastDES: A New Look of Data Encryption Standard. *International Journal of Computer Applications,* 975**,** 8887.

KUMARI, P., BALA, M. & SHARMA, A. 2017. A Comparative Study of Symmetric Key Algorithm DES AES and Blowfish for Video Encryption and Decryption. *International Journal of Advance Engineering and Research Development,* 4.

MANIKANDASARAN, S. 2016. Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage. *IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN***,** 2249-9555.

MOGHADDAM, F. F., KARIMI, O. & ALRASHDAN, M. T. A comparative study of applying real-time encryption in cloud computing environments. 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), 2013. IEEE, 185-189.

NAFI, K. W., KAR, T. S., HOQUE, S. A. & HASHEM, M. 2013. A newer user authentication, file encryption and distributed server based cloud computing security architecture. *arXiv preprint arXiv:1303.0598*.

PRAKASH, G., PRATEEK, M. & SINGH, I. Data encryption and decryption algorithms using key rotations for data security in cloud system. 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), 2014. IEEE, 624-629.

RAJORIYA, P. & MOHOTA, N. 2017. REVIEW ON FPGA IMPLEMENTATION OF IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM ALONG WITH KEY ENCRYPTION.

RATNADEWI, R., ADHIE, Y. H., AHMAR, A. S. & SETIAWAN, M. Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). J. Phys. Conf. Ser, 2018. 12009.

SHARMA, N. 2017. A Review of Information Security using Cryptography Technique. *International Journal of Advanced Research in Computer Science*, 8.

SIR, H. F. 2017. Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish. *Global Journal of Computer Science and Technology*.

SIVASANKARI, N., RAMPRIYA, K. & MUTHUKUMAR, A. 2017. Implementation of Area Efficient 128-bit Based AES Algorithm in FPGA. *European Journal of Advances in Engineering and Technology*, 4**,** 541-548.

STALLINGS, W. 2011. *Cryptography and Network Security Principle and Practice*

TEJA, T., HEMALATHA, V. & PRIYANKA, K. 2017. Encryption And Decryption–Data Security For Cloud Computing–Using Aes Algorithm. *SSRG International Journal of Computer Trends and Technology*.