THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Comprehensive Study on AES and RSA Security Algorithms in Cloud

Roopam, Manpreet Dhindsa,Harshpreet Kaur
Department of Computer Science Engineering
Lovely professional university
Jalandhar, India
Roopam.23828@lpu.co.in

Abstract—Cloud Computing referred as revolutionary approach which has changed the IT and business integration. It has benefits to almost every type of IT requirement, it can be used by enterprises to cut their IT costs, and it can be used by individual to use it as a storage solution with a disaster recovery solution. One major problem that exists with Cloud Computing, in the present scenario, is security and privacy of the data. Encryption is the most important part of the security if you own a private cloud holding your personal or critical data. It brings confidentiality to the critical data. This paper mainly reviews on existing security algorithms "Advanced Encryption Standard (AES)" and "Ron Rivest, Adi Shamir, and Adleman (RSA)".

Keywords— Cloud computing, cloud data security, AES, RSA.

I. INTRODUCTION

Associations use cloud in an assortment of different help models which incorporate "(SAAS) Software as a Service, (PASS) Platform as a Service and (IAAS) Infrastructure as Service". These administrations could be conveyed utilizing different arrangement models, the sending models are private, open and half and half. At the present time, there is no need to carry local hardware systems all over the place, it all can be handled by the cloud as an alternative. However, there is a risk that private information in these spaces can be seen by other people. This can happen in several ways like changing the settings on a document, accidentally share it with wide range of users. If a member of your group has a weak password and someone guesses that password then, any information shared with that person will be exposed, thus providing security to the data on cloud.

There are various security factors related with cloud computing. These components are partition into two main types: issues that looked by cloud suppliers and issues that looked by clients of a cloud. For the most part, cloud giving associations which is (SAAS) or (IAAS) utilize the component of a cloud. In the vast majority of cases, supplier of cloud guarantees that foundation is secure which is disseminated by supplier and customer's information and applications gave to client are ensured, additionally the client guaranteed the supplier offered the best possible security which is secure their data

II. EXISTING ALGORITHM

AES ALGORITHM

"The Advanced Encryption standard or AES" Recall that a major Shortcoming of DES is that the keylength is only 56 bit and that is considered to be short. In Other words, the key space is relatively small , and an attacker can use brute force to find the key. There was a need for a new encryptipn algorithm that have longer key length, but also be efficent. So, in 1997 NIST put out a public call to replace DES . After a few rounds of submissions and reviews, AES was finalized and it became a new standard.Like DES ,AES is also a block cipher, whereas in DES,the input plaintext block is 64 bit in AES it is 128 bit. In DES the keylength is only56 bit .In AES it can be 128,192 or 256 bits.These key lengths are considered long enough to defeat brute force attempt to search for a key [5][7] .

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

A. OPERATIONS

The plaintext square is meant as a square network. Consider it a state exhibit, and first XOR with the key. Again the Key is likewise implied as a square lattice. At that point the state clusters experience numerous of encryption. At each round it experiences a few activities that, speak to substitution and stage and furthermore the round key is Xor, to this state cluster .The activity at each round incorporate substitute bytes. This includes utilizing a table expressed to as a Sbox to accomplish byte substitution of the square. Move lines is a basic plan that is push by push. Blended segments is a substitution that adjusts every byte in a segment as utility of the bytes in the section and afterward the outcome is XOR in a round key. The procedures of the last round incorporates "Substitute bytes, Shift columns and Add round key", and the result is a figure content.

In AES, the unscrambling technique runs the calculation in the invert bearing. This implies every one of these procedures must be reversible. A XOR activity without anyone else's input is reversible. Different tasks signifying "Substitute Bytes, Shift Rows and Mix Columns", and converse capacity is utilized in a decoding calculation. By utilizing this opposite capacity, it can turn around the activity of substitute bytes that was performed in the encryption. In like manner, it can switch the impacts of move lines and blend sections in the decoding procedure. Accordingly, every one of the procedures are reversible. Thus, when we run the calculation in the turnaround request, we can unscramble the figure message once more into the plaintext. ENCRYPTION PROCESS.

AES encryption consist of four sub-processes.

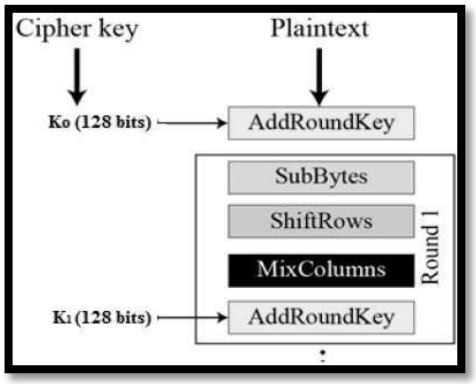

Figure1.Encryption Process

a) Byte Substitution (Sub Bytes)

In AES divided 128 bits inputs in 16 input bytes, these input bytes divided for a S-box. S-box gives results in matrix form in which have four by four rows and columns.

b) Shift rows

In shift rows process, shift the each row of given matrix to the left. On the right side of row, re-inserted the entries which are 'fall off'. Process for shift rows are:

First row of known matrix does not shifted by this process. Second row shifted to the left at one position. Third row shifted at two positions to the left side. Fourth row of matrix shifted at three position to left side. In which only shift the rows, input bytes is no change in new matrix.

c) Mix Columns

In mix column process, used special mathematical function for transformation of each column consist of four bytes. In this function four bytes of single column as input and outcome is four new bytes, which is replaced with original bytes of column. This process gave new matrix which is consist 16 new bytes. This process does not perform in last round of AES.

d) Add round key

In this process, matrix of 16 bytes consider as 128 bits and perform XOR operation to these 128 bits of round keys. In the last round output of this in the form of cipher text and 128 bits also change in 16 bytes.

B. Decryption Process

Reverse process of encryption process is similar to decryption process of an AES. In which four processes performed in each round in a reverse order. These processes are: 'Add round key', 'Mix columns', 'Shift rows', 'Byte substitution'

Each round also consist sub-processes which are also in reverse order. Encryption and Decryption algorithms implemented separately.

C. AES Analysis

In present day, AES used cryptography, which is supported by hardware and software. Practically performed, in AES does not find cryptanalytic attacks against AES. Also, AES has key length flexibility which helps for 'future proofing' with ability to performed extensive key searches.

AES algorithm only guaranteed when this is correctly applied and provided good key management.

RSA ALGORITHM

RSA is a Cryptographic Algorithm utilized for encoding information over the system. It was found by "Ron Rivest, Adi Shamir, and Adleman in 1978". It is a sort of hilter kilter key based calculation that utilizations two keys which is "Open key" and "Private key". Open key is produced for the most part encoding the message (There is the other path around as well, known as Digital Signing) and Private Key for unscrambling the message. For encrypting, the receiver has to send his public key to the sender so that only the receiver will be able to decrypt it using private key. It is highly secure and reliable due to large prime numbers and their multiplication. But also is difficult to maintain due to complex numbers generation and even loss of data [12].

A. How does it work

Any user wants to use RSA, must create two Keys:

a) Public Key, anyone can see this Key.
b) Private Key, only the owner can see this Key.

If A needs to send a message to B, it can be followed by two methods.

First Method

1. A, encrypts his message with his private key.
2. B, decrypts the message with the public key of A.

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Second Method
1. A, encrypts his message with the public key of B.
2. B, decrypts the message with his private key.

B. Generate the Keys

To generate the keys we need to follow these steps:

a) Consider two prime numbers A and B;
b) 2. Calculate N = A * B;
c) 3. Calculate Z = (A – 1) * (B – 1);
d) Choose a private key (It mustn't have common factors with Z and must be less than Z);
e) Calculate the public key knowing that (Private Key * Public Key) mod Z = 1.

C. Example

Choose two prime number s A and B:
A = 11
B = 17
Calculate N = A * B:
N = A * B = 11 * 17 = 187`
Calculate Z = (A – 1) * (B – 1) :
Z = (A – 1) * (B – 1) = (11 – 1) * (17 – 1) = 10 * 16 = 160
Choose a private key (It must not have common f actors with Z and must be less than Z):
Private Key = 3
Calculate the public key knowing that (Private Key * Public Key) mod Z = 1:
(3 * Public Key) mod 160 = 1
Public Key = 107
Public Key = (107, 187)
Private Key = (3, 187)

D. Encrypt a Message

To encrypt a message, consider alphabet, like this:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 2. Alphabet with key

Then, encrypt a message with the FIRST METHOD (Encrypt with the public key of A and decrypt with the private key of A)

CLEARTEXT	**M**	**M^3 mod 187**
S	19	127
I	9	168
S	19	127

T	20	146
E	5	125
M	13	140
I	9	168

Table 2. Encryption of Clear text

E. Decrypt a Message

To encrypt a message use the FIRST METHOD of encryption, so, decrypt the message with the public key of A:

ENCRYPTED TEXT (C)	**C^{107} mod 187**	**DECRYPTED TEXT**
127	19	S
168	9	I
127	19	S
146	20	T
125	5	E
140	13	M
168	9	I

Table 3. Decryption of Encrypted Text

III. COMPARATIVE ANALYSIS OF AES AND RSA

TABLE 4. COMPARISON OF EXISTING CLOUD SECURITY ALGORITHMS BASED ON SEVERAL PARAMETERS

PARAMETER	**ALGORITHM**	
	AES	***RSA***
Developed	2000	1978
Key size	128,192,256 bits	1024 bits
Block size	128 bits	Minimum 512 bits
Ciphering and Deciphering key	Exact Same	Different
Algorithm	Symmetric algorithm	Asymmetric Algorithm
Encryption	Faster	Slower
Decryption	Faster	Slower
Power Consumption	Low	High

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

PARAMETER	ALGORITHM	
	AES	***RSA***
Security	Excellent Secured	Compared Secured
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced and Oracle attack
Key	For Encryption and Decryption Similar key is used	for Encryption and Decryption Different is key used
Rounds	10,12,14	1
Hardware and Software Implementation	Faster	Not Efficient
Ciphering and Deciphering Algorithm	Different	Same

IV. CONCLUSION AND FUTURE WORK

AES used to encode files and document, it is the fast and secure algorithm. AES uses the same key for Encoding and Decoding. There is key exchange problem, because if communication is done by AES then the receiver has to have a key. This problem overcome by using asymmetric algorithms which is RSA, in this encryption is done by sender's side with the help of Private key and decryption is done by receiver's side with the help of Public key to decrypt that encoded message. AES can be applied with relatively simple bit operations but RSA includes mathematics with very large numbers. RSA is more secure, but they utilize more CPU and memory resources than AES. There were still some of the problems related to present security algorithms such as "Timing attacks and problems with key distributions" and looking for more sophisticated algorithms of AES, RSA.

REFERENCES

[1] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[2] B. Schneier, " Description of a New VariableLength Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption", Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[3] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

[4] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.

[5] 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.

[6] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.

[7] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[8] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[9] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[10] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.

[11] S. K. Randeep Kaur, "Analysis of Security Algorithms in Cloud," International Journal of Application or Innovation In Engineering & Management(IJAIEM), vol. 3, no. 3, 2014.

[12] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[13] 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