Study of Cloud Computing Security Methods: Cryptography

Maryann Thomas[#1], S. V. Athawale[*2]

[#]Student ,Department Of Computer Engineering,AISSMS COE,1, RB Motilal Kennedy Rd, Railway Officers Colony, Sangamvadi, Pune, Maharashtra,India

Abstract

Data can be stored on the internet or cloud, so that clients can access their data or applications anytime and anywhere through any device connected to the Internet. This is called Cloud Computing.

It provides on-demand access, and reduces the need for advanced hardware thereby making it extremely convenient for clients.

With the rising popularity of cloud based services, the frequency of malicious attacks on cloud storage and data leaking is also rising. It is important to protect the user's data privacy. Thus it has become extremely crucial to ensure security in cloud storage.

One of the methods to protect the data is cryptography. Cryptography is a method in which data is converted into a meaningless form so that unauthorized users cannot read it. Data can be encrypted by various algorithms. It destroys the format of the data as well as the look and feel of it , the length of data may also increase due to added padding.

During decryption,the added padding is stripped off and the encrypted data is decoded so that it returns back to its original form.

Keywords - *cloud computing, data privacy, security, cryptography*

I. INTRODUCTION

Cloud computing is an Internet-based computing model which provides several online resources to clients on demand basis, without buying the underlying infrastructure. [1]

Cloud based services are being widely used and accepted all over the world. Nowadays,the use of internet for data storage and online applications has become pivotal for industrial ,commercial as well as domestic establishments. Types of services that are provided by the cloud are SaaS(Software as a Service),PaaS(Platform as a Service) and IaaS (Infrastructure as a Service). These services may be provided to clients on pay-per-use ,subscription, monthly rental basis,etc. Though these are cheap and convenient ,they are not free from threats and attacks . Cryptography is one of the methods to obtain security in cloud.There are 3 types of cryptographic algorithms :Symmetric key algorithms, Asymmetric key algorithms and Hashing.Symmetric Key Algorithms use a single key for encryption and decryption, while asymmetric algorithms use different keys. Hash Algorithms compress data for signing to standard fixed size [2].

In this paper, we are going to discuss Cryptography algorithms : DES, 3-DES and AES and how they are useful to secure the cloud. Both of these algorithms are symmetric key algorithms. They will be described in the following sections.

II. DES ALGORITHM

The Data Encryption Standard Algorithm is a block cipher algorithm, which means that the data is processed in blocks i.e. the encryption and decryption processes are carried out on these blocks. The plain text is converted to ciphertext in a number of blocks,each of size 64 bits.It follows the Feistel Structure. According to the Feistel Structure, the encryption is carried out in a number of rounds, and each round requires an independent subkey. The plaintext is processed in 16 rounds. The key size is 64 bits which is later converted to 56 bits.[3]

Since there are 16 rounds in DES, 16 subkeys are required each of size 48 bits which are generated from the original key. Cipher text generated will be in a block of size 64 bit. The steps in this algorithm are depicted in Fig 1.

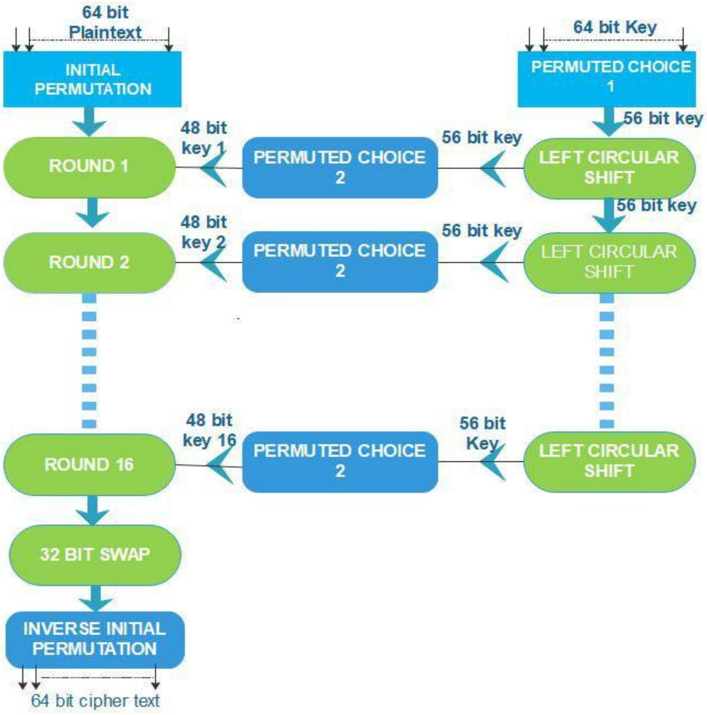

Fig 1 : DES ALGORITHM

First,the 'Initial permutation' is applied to the 64 bit plaintext, where the bit positions of the block are rearranged according to a predefined transposition order. The 64 bit output is given as an input to Round

1. A subkey is required to execute the round, so parallelly a subkey is generated. For this ,a 64 bit original key is given as input to the function 'Permuted Choice 1' which gives the output as a 56 bit key.Now Left Circular Shift is applied to that 56 bit key. The number of bits to be shifted is determined by the round number. Then 'Permuted Choice 2' operation is applied to that 56 bit key ,where reshuffling of bits is performed according to a fixed transposition order. It reduces 8 bits and gives a 48 bit subkey. This key is then given as an input to Round 1. Similarly , a total of 16 rounds are executed. After completion of these rounds, a 32 bit Swap is performed; the 64 bit output is divided into 2 halves and they are swapped. Finally, 'Inverse Initial Permutation' is performed which is again a reshuffling of the bit positions according to a fixed transposition order. The output from this is the required 64 bit Ciphertext.

Processing in each round

The 64 bit input is divided into 2 halves: left and right, each having 32 bit length. The key is also divided into two halves: each having length 28 bit. Expansion Permutation operation is implemented on the right half of the input text, which adds 16 more .bits to it, making it 48 bits . These 48 bits are XORed with the key

Left Circular shift is performed is performed on both halves of the key separately , and then given as input to a Contraction function(Permuted Choice-2). The 48 bit output from this is XORed with the previously discussed 48 bits from the Expansion Permutation operation . The result of this operation is given as input to Substitution box, which gives a 32 bit output , on which a Permutation operation is applied, which gives a 32 bit output. This output is XORed with the left half of the original input and the output from this is stored as the right half and the original right half is stored as the left half. this will be the input given to the next round.

The DES algorithm provides weak security and is unsafe as the key size is too small and it is vulnerable to brute force attacks. In January 1999 distributed net and the Electronic Frontier Foundation (EFF) collaborated to publicly break a DES key in 22 hours and 15 minutes[4]. To overcome this, Triple DES algorithm was created.

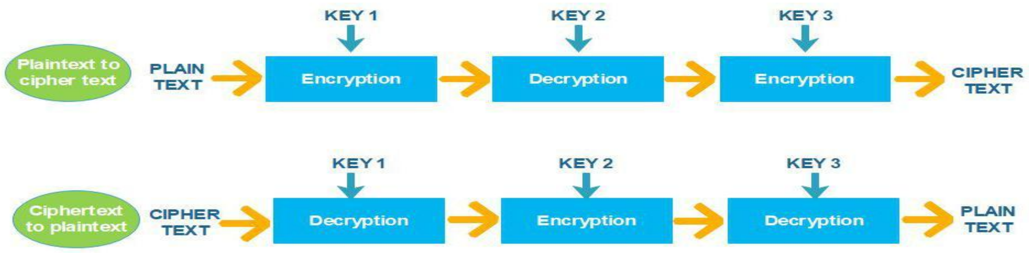

FIG 2 : Triple Des Algorithm

III. 3-DES ALGORITHM

The DES Algorithm is a 56 bit Cryptography Algorithm. To increase the key size and the security , we can apply the DES algorithm multiple times.

In the Triple DES algorithm, the DES Algorithm is applied three times. First the plain text is encrypted using a key , decrypted using a different key and then encrypted again to get the final cipher text.

When ciphertext is to be converted back to its original form, it is decrypted first, then encrypted using a different key and then decrypted again.[5] When the first key is taken the same as the third key, we obtain a 112 bit cryptography , and if all three keys are taken different, we can obtain 168 bit cryptography.

If we take the first key same as the second key, the encryption and decryption will cancel each other out , and the result will be the same as that of simple DES Algorithm with a 56 bit key which is the third key.

IV. AES ALGORITHM

subkeys are used in the Pre-round Calculation, making it a total of 44 subkeys. The ciphertext generated is of size 128 bit. The working of this algorithm is shown in Fig 3.

The 128 bit block of plaintext is given as input to the ‘Add Round Key’ operation ,which is an XOR operation, where the plaintext is XORed with 4 subkeys : K0 [w0...w3]. This operation is a pre-round calculation: it is executed only once at the beginning and not repeated in every round.

The result is sent to the operation 'Substitution Bytes'.

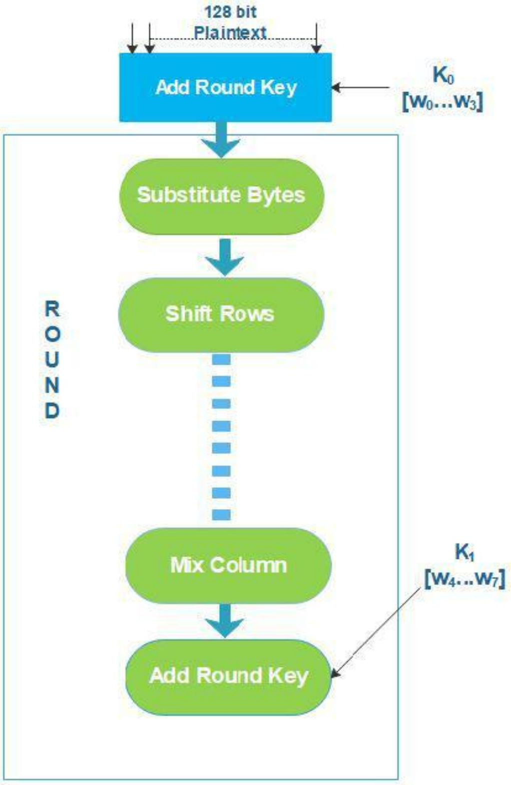

Fig 3 : AES Algorithm

The Advanced Encryption Standard Algorithm is also a block cipher algorithm. There are three variants of this algorithm according to key sizes: 128 bit, 192 bit and 256 bit key versions.[6]

The number of rounds in the AES algorithm will be decided by the key size. In this paper we will discuss the 128 bit version. The block size of plaintext is 128 bits and it is processed in 10 rounds. The 128 bit key is considered as a total of four words where one word represents 32 bits. The total number of subkeys required is 44, where each subkey is of 4 bytes (one word). Four subkeys are required in each round ,so a total of 40 subkeys is required. Another 4

The AES S-Box implements inverse multiplication in Galois Field 28.[6]

The output from this is given as input to 'Shift Rows',which is nothing but Circular Right shift operation. The next function ,'Mix Columns', multiplies the input with a predefined matrix.The output from this is sent to 'Add Round Key', where again the next four subkeys are used :K1 [w4...w7]. This operation is part of a round, and it is executed 10 times, using the subsequent subkeys. In Round 2, the subkeys K2 [w8...w11] will be used, in Round 3, the subkeys K3 [w12...w15] will be used and so on .

In the last round, the 'Mix Column' operation is skipped. After 10 rounds are completed, 128 bit block of ciphertext is obtained.

IV.COMPARISON OF AES AND 3-DES ALGORITHMS

Both of these algorithms are symmetric block cipher algorithms. The AES algorithm is more effective in providing security than the 3-DES algorithm.Data Encryption Standard (DES), the algorithm 3DES is based on, was retired in 2005 and the two-key variant of 3DES was retired in 2015[7]Triple DES was implemented because the DES Algorithm was proven to be vulnerable to brute force attacks. But later, even Triple DES was proven ineffective against brute force attacks.According to draft guidance published by NIST on July 19, 2018, 3DES is officially being retired . The guidelines propose that Triple DES be deprecated for all new applications and disallowed after 2023.[8] Thus we could say that 3-DES will soon become obsolete.

TABLE I
Difference between AES and 3-DES Algorithm

	AES Algorithm	**3-DES Algorithm**
Network used	Based on the substitution-permutation network	3-DES is just an adaptation to the older DES encryption that relied on the balanced Feistel network
cryptanalysis resistance:	AES is strong against differential, linear , interpolation and square attacks	3des is vulnerable to differential cryptanalysis
Encryption key lengths	AES uses three common encryption key lengths, 128, 192, and 256 bits	3DES can have encryption key lengths of 168, 112, or 56 bit lengths
Block length	Block length is 128 bit	Block length is 64 bit

Year of Introduction	Introduced in the year 2000	Introduced in the year 1977
Repetition of Encryption keys	All encryption keys must be distinct	Encryption keys may or may not be repeated
Speed	AES is faster than 3-DES	Running same process thrice is time consuming so 3-DES is slower
Security Provided	Strong security	Inadequate and vulnerable

V. CONCLUSION

With the growth of technology and development of advanced computers,it has become easier for hackers to gain unauthorized access to confidential data. Thus it has become essential that reliable security methods be developed to match the ever-evolving technology. Since cloud based services are gaining fast popularity, proper security for clients' data is the need of the hour. Cryptography is one of the most complex methods to provide security.

In this paper we have discussed the most popular cryptographic algorithms :AES, DES and 3-DES and their working in a concise manner. We have also discussed the basic differences between them . The DES and 3-DES algorithm,though easier to implement, have proven to be vulnerable ,and the AES algorithm is our best bet when we need to secure data.

As security is the need of the hour in today's world,there is a lot of scope for future research on this topic.

ACKNOWLEDGEMENTS

I would like to thank Prof. Mr. S.V. Athavale Sir, who inspired and guided me in formulating this paper. I would also like to express my gratitude to family and friends for their constant motivation and support.

REFERENCES

[1] Rishav Chatterjee, Sharmistha Roy,Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud ,Volume 7 Issue No.5 , 2017 IJESC

[2] Akashdeep Bhardwaja,GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd ,Security Algorithms for Cloud Computing,Elsevier,International Conference on Computational Modeling and Security (CMS 2016)

[3] CCM website [online]: https://ccm.net/contents/134-introduction-to-encryption-with-des

[4] Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technol. 3(2): 1-7. DOI: 10.15226/2474-9257/3/2/00132

[5] ComputerHope website [online]: :https://www.computerhope.com/jargon/num/3des.htm

[6] Commonlounge website :https://www.commonlounge.com/discussion/e32fdd267aaa4 240a4464723bc74d0a5

[7] Cryptomathic website [online]: /www.cryptomathic.com/news-events/blog/3des-is-officially-being-retired

[8] Syncsort website [online]: https://blog.syncsort.com/2018/08/data-security/aes-vs-des-e ncryption-standard-3des-tdea/