IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 13-17

Comparative Analysis of algorithms while encrypting data in Cloud

Shivam Agarwal[1], Tanuja Bodas[2], Dr. Bharati Wukkadada[3]
[1]*(Student MCA, K. J. Somaiya Institute of Management Studies and Research, Mumbai)*
[2]*(Student MCA, K. J. Somaiya Institute of Management Studies and Research, Mumbai)*
[3]*(Assistant Professor IT, K. J. Somaiya Institute of Management Studies and Research, Mumbai)*

Abstract: *This paper talks about data security, when confidential information is revealed into an undesirable environment intentionally or unintentionally, it is known as a data breach. This paper concern regarding stored data, the way it is encrypted and the problems faced during decryption. This paper aims to increase the time complexity to decrypt data using the RSA algorithm over various other algorithms like DES, AES, and IDEA along with concepts of factorization.*
Keywords: *R.S.A. algorithm, D.E.S., A.E.S., I.D.E.A.*

I. Introduction

In the era of modern world, varied services provided on the internet as a traditional hosting. Memory storage and system usage are fixed in these traditional kinds of systems. Quick retrieval of data from any place and at any point of time i.e. portability has become the need of the hour. Database is a successful cloud service. The cloud infrastructure contains storage devices and database engines which is transparent to the application owner. These services are distributed anywhere across the globe. The application owner stores data. However, the major concern is the security and concealment of data. Securing data is always of crucial importance and because of the critical nature of cloud and the large amounts of complex data it carries, the needs are even more important. The cloud storage is reliable and powerful, but there are a wide range of external as well as internal threats for storing data on the cloud. This information is secured by the means of Public key and Private key.

A key which is public shared with everyone and the decryption of this data with a special key which is private, which is known only to the user.

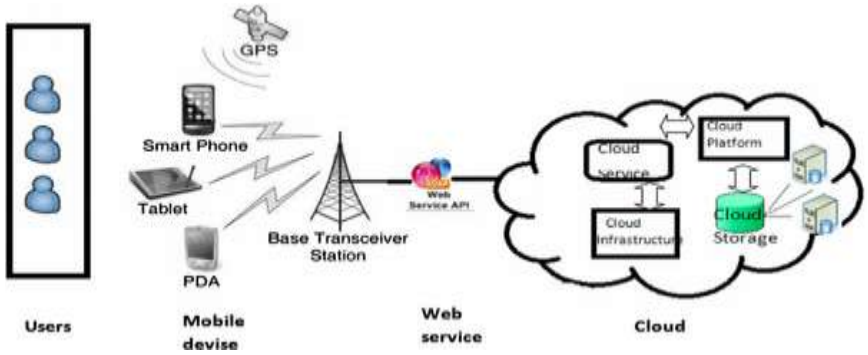
Encryption is a probabilistic algorithm designed by researchers or encryptions in which plain text (Tp) will encrypt in encrypted text (Te) by using a public key(Pk2) and private key(Pk1).
Decryption is an algorithm designed by person who is decrypting it. The algorithm inputs the encrypted text (Te) and decrypt it to plain text (Tp) by using Pk1 and Pk2.

A.E.S, D.E.S., R.S.A. and Triple D.E.S. etc. are popular symmetric or Asymmetric Key Algorithms. One of these algorithms are used for encryption. The encryption and decryption procedures are done using the a-symmetric key algorithm which is RSA using different keys for encryption and decryption. Encryption can be made powerful by using varied Key Size. Therefore, attackers find it problematic to hack such kind of data. The Key size and the time taken for encryption and decryption are directly proportional. In the Algorithm given in this paper, the time of encrypting and decrypting data is reduced by when the file is divided into portions and the strength of the process is enhanced when the size of the key is increased. Hassle-free storage of data into the cloud by the user is allowed because of this.

II. Related Work:

- **Cloud Storage Architecture**

Cloud Storage Architecture: It includes multiple Cloud Components [3] like public cloud, private cloud, community cloud, interacting with each other over application interfaces, usually web services. There exists a combination of all the three cloud storages known as hybrid cloud. Web browsers and/or software applications access to cloud applications when the Cloud architecture is expanded to the client side.



Figure(i): Cloud-Architecture (source: https://www.google.co.in/)

- Rivest Shamir Adleman (RSA)[5] had proposed this algorithm in their paper 1977. R.S.A is used as a-symmetric key and the strong one encryption algorithm. R.S.A, one of the oldest public key encryption algorithm. Here, the public key is used for encoding data. Basic defined fact is to find the prime numbers since it is difficult to factorize the prime number and finds the factors of it. A typical size of key is 1024bits, used by R.S.A. for encryption and decryption. R.S.A. algorithm picks out 2 numbers which are prime, arbitrarily and multiplies to get result a fresh composite number. After evaluating the composite(result) number, it generates the key. An arbitrary number is taken out from the range, given to the prime number. The public and personal (or private) key pairs are created based on the Key term.
- D.E.S.
  Data Encryption Standard (DES) [4] is a Symmetric key algorithm which works in blocks. It uses key's size of 56bits to encode the simple text block of 64bits size.
  This algorithm uses nineteen rounds, every round uses a series of Substitution-Boxes and Permutation Boxes also called S-Box and P-Box and eXclusive OR also called XOR operation. This algorithm is prone to Brute-Force Attack and Differential-Cryptanalysis attack, so it not a very reliable algorithm
- A.E.S.
  Since D.E.S is a weak algorithm, it is prone to various attacks, a new algorithm was developed by National-Institute-of-Standard and Technology called the Advanced-Encryption-Standard also called A.E.S. A.E.S. has three versions. A.E.S. having block size 128 bit, it uses 10 rounds, AES having 192 bit block size, uses 12 round and AES having block size 256 bit, uses 14 rounds. The following steps are involved in each round- swap-byte, shift-rows, mixed-columns and add-round-key.
  A.E.S. Algorithm is more protected than any other algorithms. S-Box is not secure which leads to various attacks. This revised algorithm overpowers the designs and computations overhead.
- I.D.E.A.[5] stands for International-Data- Encryption-Algorithm was invented in 1990 by James Massey and Xuejial Lai in their paper. It uses the 128bit key, encrypts block of 64bit text which is in its original form to 64bit block Encrypted Text. I.D.E.A. includes 8-rounds and 4-final transformations. To bridge the gap in the Data Encryption Algorithm, the IDEA 128-bit algorithm is used.

III. Findings:

Comparative Analysis of Algorithms[4]

Algorithm & Year	Size of Block (in Bits)	key length (in Bits)	Number of Cycles	Level of Security	Attacks Vulnerable
DES (1977)	64	56	16	Not adequate	brute Force, Differential attack, (MIM) Man in Middle attack
3-DES (1978)	64	112 – 168	48	Vulnerable	Brute force, Differential Attack
IDEA (1991)	64	64 – 128	5 – 8	Vulnerable	Linear-Attack
AES (2000)	128	128 - 256	10 – 14	Excellent	Side-Channel attack
RSA (1977)	Not-Fixed	>=1024	Nil	Very High	brute Force and Timing-Attack

The above table shows the comparison between various algorithms of encryption according to their block size, length of the key in bits, number of cycles required to encrypt data, level of security, and the attacks it is vulnerable to.

D.E.S., 3-D.E.S., and I.D.E.A. have t6he same number of block-size but the length of the key in DES is 56 bits which is why it takes just 16 of cycles to encrypt a piece of text. Due to this, the level of security is enough to defend itself from attacks such as Brute-force, Differential Attack, Men in the Middle attack also called MIM. Whereas 3D.E.S. has key length between 112 to 168 and the number of rounds required to encrypt data is 48 which is still not enough since it is susceptible to Brute-Force and Man In the Middle attack just like D.E.S. Same is the case with the I.D.E.A. algorithm. Though it has a block-Size of 64 bits, it just takes 5 to 8 rounds to encrypt the data. The lesser number of rounds make the algorithm susceptible to Linear Attack.

A.E.S. and R.S.A. are powerful algorithms as compared to DES, 3DES, IDEA. The block-size in AES is double as that of DES,3DES, IDEA which is 128 bits. Since the block-size is double the length of key required to encrypt the data is also double which is between 128 and 256. This directly affects the number of cycles it will take which is between 10 and 14. All of this results in an excellent level of security. But, this is not enough. It is still susceptible to Side-Channel Attack. Side-Channel Attacks are implemented by whatever information is using the available data. But, when it comes to RSA, the block-size is not fixed nor is the key length. The only condition regarding the length of the key is that it has to be equal to or less than 1024 bits. Since the number of cycles depends on the block-size and the key length which is variable, the number of cycles is also variable. This makes the level of security very high but it still susceptible to Brute-Force and Timing-Attack.

IV. Implementation:

IV.I. Proposed Work

In our proposed work, talks about the time taken to encrypt and save data in a cloud storage. To achieve this, we have used RSA algorithm with AES, DES and IDEA.

IV.II. Process of Encryption and Decryption

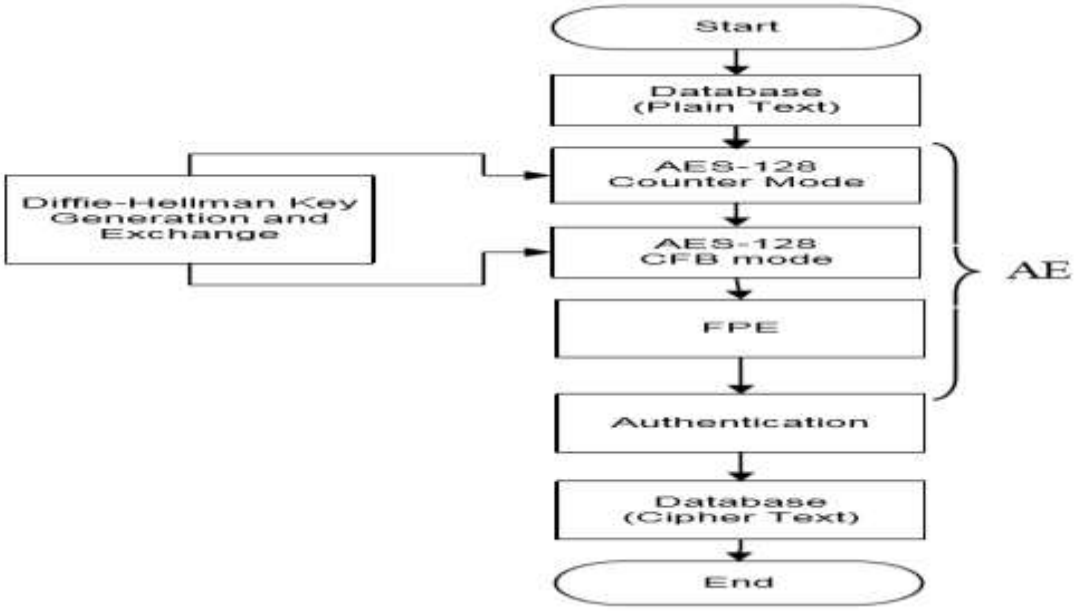


Figure.(ii): Encryption Procedure[6]

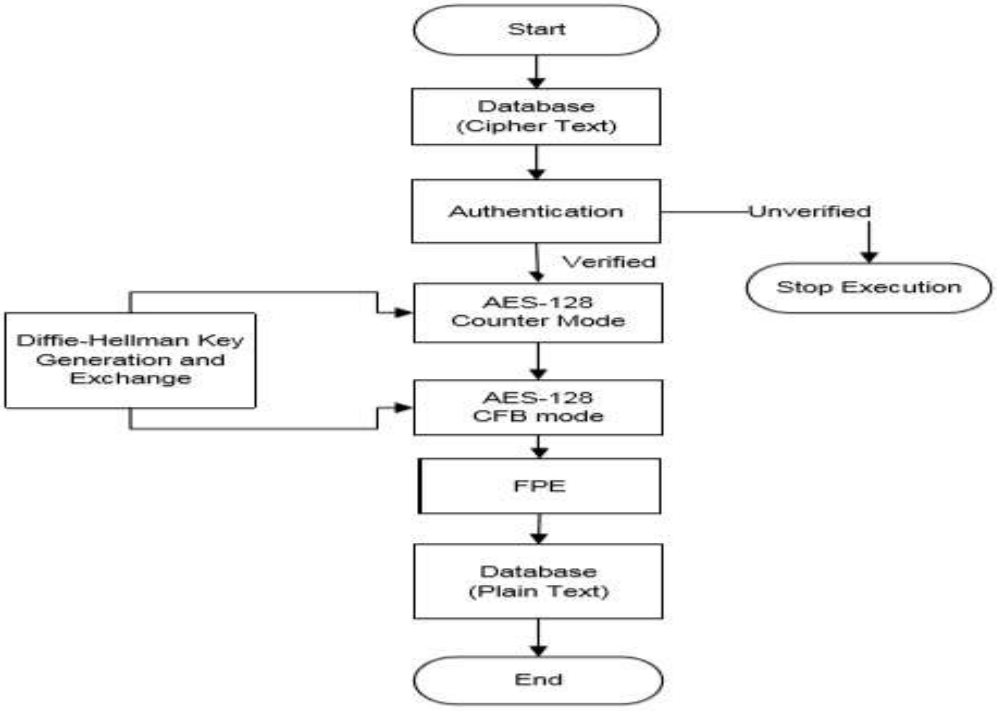


Figure.(iii): Decryption Procedure[6]

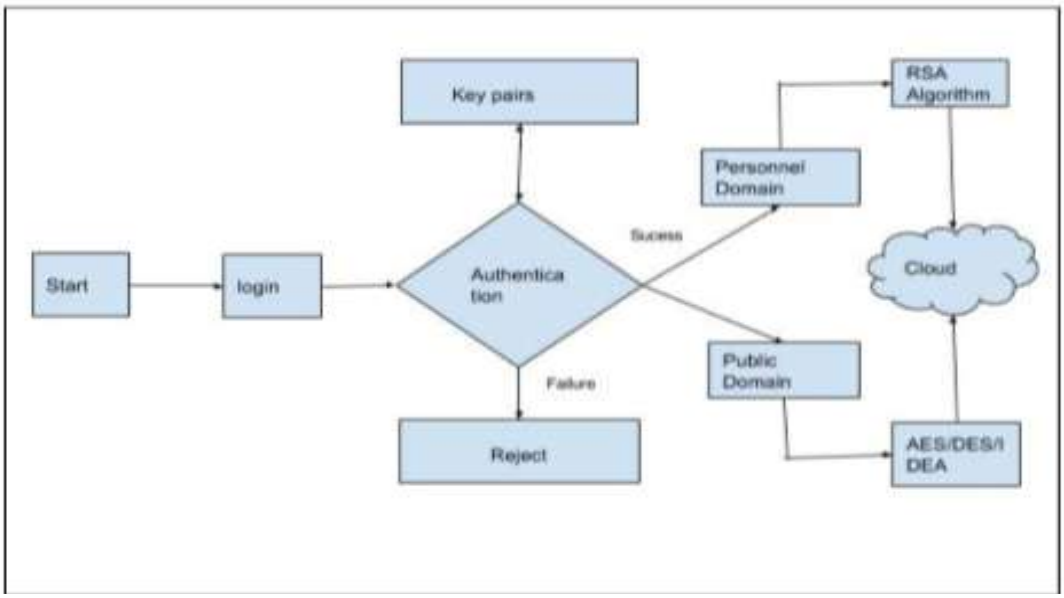


Fig.(iv): Encryption of data in Cloud[5]

V. Conclusion:

We have made a performance analysis of various algorithms when put together. For this, in private domain we are using R.S.A. algorithm for encryption purpose.

R.S.A. with D.E.S. [5]

D.E.S. has the same key for encryption and decryption. Any communication between the sender and receiver can be done using different keys and the key can be exchanged. If R.S.A. is used for encrypting the key separately, then the receiver can use D.E.S. for encrypting and decrypting the message.

R.S.A. with A.E.S.

R.S.A. has two keys; one key is private, and one key is public. A.E.S. is faster and more secure. For its encryption and decryption is uses the same key. The receiver must have the key, so there appears the problem of

Key Exchange. The solution to this problem is solved the R.S.A. The sender sends the message using a private key. Receiver decrypts the message with the public key.

C. R.S.A. with I.D.E.A.

In public domain I.D.E.A. encryption algorithm is used for the purpose of encryption. There are many clients in the public domain, so the method shown brings together all the available clients.

References

[1]. Dr. D.I. George Amalarethinam, H. M. Leena, *Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud*

[2]. Ying-yu Cao, Chong Fu ,*An Efficient Implementation of RSA Digital Signature Algorithm*

[3]. PachipalaYellamma, ChallaNarasimham, VelagapudiSreenivas; *Data Security in cloud using RSA*

[4]. Pradeep Semwal, Mahesh Kumar Sharma, *Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing*

[5]. Krishna KeerthiChennam, Lakshmi Muddana, RajaniKanth, Aluvali, *Performance Analysis of various Encryption Algorithms for usage in Multistage Encryption for Securing Data in Cloud.*

[6]. Zalak Bhatt, Prof. Vinit Gupta, *Advanced Security Technique for Format Preserving Encryption*