IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Survey on Public Key Cryptography for Securing Data in Cloud Computing

M.Keerthika[1], K.Indhumathi[2], V.S.Lakshmi Priya[3], T.Fathima Barveen[4]

II MCA, Anjalai Ammal Magalingam Engineering College, Kovilvenni[1-4]

Abstract: Cloud computing provides convey of computing services such as networking, storage, databases, servers, databases, software, analytics and Online Internet . Cloud computing as a favor can transform and attract Information technology services. Now days, security of data become a large concern to insure various aspect like integrity, confidentiality, authentication etc. Cryptography techniques are used for this purpose. It plays a major role in protecting the data in those applications which are running in a network environment. To increase data security cryptography techniques also used on cloud because cloud computing provides secure transmission of data. On cloud, various computing task or programs can be run at a time. Cloud computing provides an illusion to the customers of using infinite computing resources that are available from anywhere, anytime, on demand.

Keywords: Cryptography, Cloud computing, RAS, DES, Ciphertext.

INTRODUCTION

The concept of cloud is not new. Network based computing is evolving for more than 50 years. But the term 'cloud' originated in 1990s. Many believe the first use of “cloud computing” in its modern context. It is a virtual environment that provides resources to users and charges only for services they consumed [8]. Security is the major issue in the adoption of cloud computing. This set of groups provide a central management for monitoring all events (upload, download) done in the cloud and classify them. Cloud typically has single security architecture but have many customers with different demands. Many cryptographic algorithms are available to solve data security issue in cloud. Algorithms hide data from unauthorized users. Data security is an important factor for both cloud computing and traditional desktop applications. This is to obtain the highest possible level of privacy. Modern Encryption algorithms play the main role in data security of cloud computing. Two operations performed by these algorithms are encryption and decryption. Encryption is the process of converting data into struggle form and Decryption is the process of converting data from struggle form to human readable form. Symmetric algorithms use one key for encryption and decryption while Asymmetric algorithms use two keys for encryption and decryption. Cloud services hold user's personal data and identity information such as photographs, calendars, address books, medical records, social security numbers, tax documents, financial transactions etc [4]. These data if analyzed properly can tell every aspect of user's life. Consider banks and other financial institutions which process highly sensitive data, if they use cloud high degree of security is required for their data.

LITERARTURE REVIEW

Nasarul Islam.K.V, Mohamed Riyas.K.V: Based on the text files used and the experimental results it was concluded that DES algorithm consumes low encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm, but RSA Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Comparison of secret key and public key based DES and RSA algorithms, it clears that RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography. But it does not solve all the security infrastructure.

TalariBhanu Teja,Vootla Hemalatha,K priyanka : Encrypt and Decrypt- As per, encrypting is the change of any sort of information into a frame that is not reasonable. Decoding is the resistance of the encrypt which changes over encoded information into justifiable frame. Keeping in mind the end goal to decode the encryption, a key which is frequently called decoding key is required for switch operations. Without a right encrypted key, a message may not be download. In such conditions, decoding must be extricated from the encryption designs be that as it may, lost the decrypted key for the most part result in loss of decoded message.

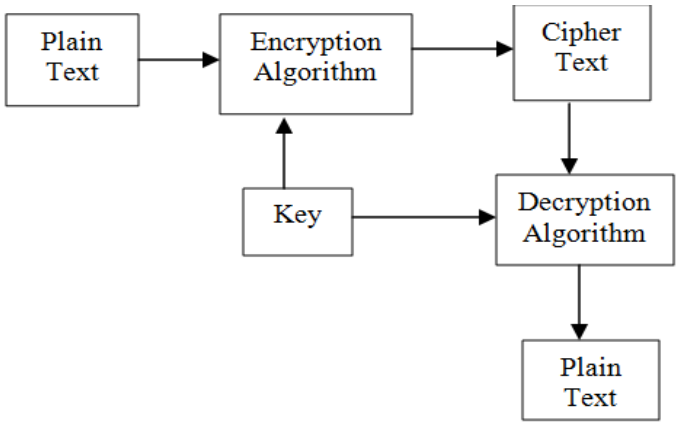
J. Athena, V. Sumathy: This paper addressed the limitations in the security assurance and the data privacy limitations with increase in size of the data on cloud. The evolution of cryptographic approaches addressed these limitations and provided the solution to the preserving process. Due to the multi-tenancy property of the cloud, server and the geographical factors limited the security of the cloud data access and storage.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

TYPES OF CRYPTOGRAPHY

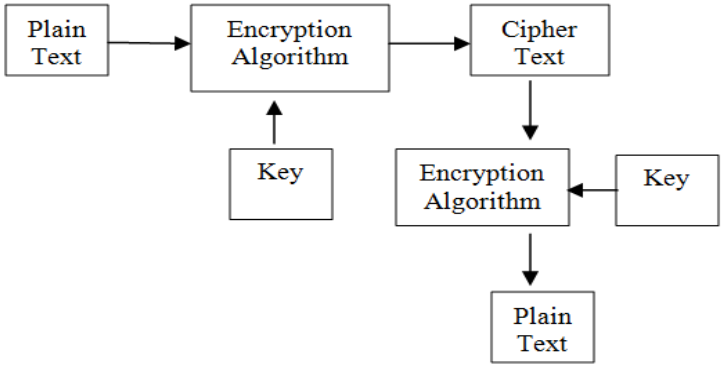
There are two types of Cryptography.

(1) Symmetric-key cryptography
In a symmetric cryptosystem, the same key is used for encryption and decryption [2, 4].



Symmetric key Cryptography
Source of Study of RSA, DES and Cloud Computing

(2) Asymmetric-key cryptography
In an asymmetric, the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key [2, 4].



Asymmetric key Cryptography
Source of Study of RSA, DES and Cloud Computing

CRYPTOGRAPHY

It is a science used to secure precise data. Confidentiality is the significant security service provided by cryptography, keeping data conceal to unauthorized users [6]. Components of cryptosystem are follows:

- **Plaintext:** Original form of data, data to be protected during transmission and storage.
- **Cipher text:** It is the unreadable form of the plaintext after encryption operation.
- **Encryption Algorithm:** Used to convert plaintext to cipher text, it is a mathematical process.
- **Decryption Algorithm:** It performs reverse operation of encryption algorithm, convert cipher text to plaintext.
- **Encryption Key:** It is a value used by sender with algorithm to convert plaintext to cipher text.
- **Decryption Key:** It is a value used by receiver with algorithm to convert cipher text to plaintext.

ENCRYPTION ALGORITHMS FOR CLOUD SECURITY:
Many algorithms are accessible for cloud security. Most convenient algorithms for cloud security are discussed below.

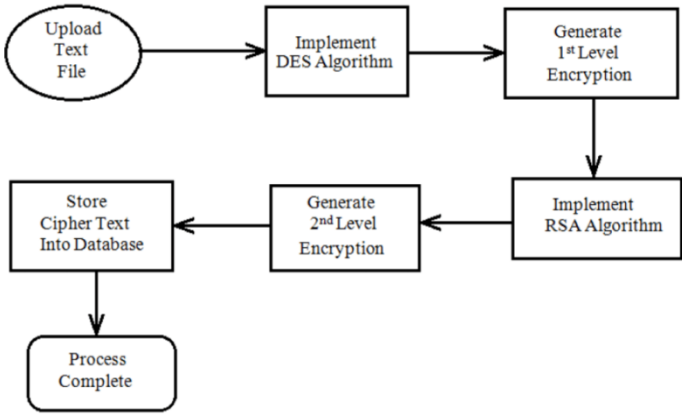
❖ **Data Encryption Standard (DES):**

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits. Entire plaintext is divided into blocks of 64bit size; last block is padded if necessary [6]. Multiple modifications and changes are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. Entire operation can divided into three phase. First phase is Initial permutation and last phase is the final permutations.

- Initial permutation rearranges the bits of 64-bit plaintext. It is not using any keys, working in a predefined form.
- There are 16 fiestel rounds in second phase.
- Each round uses a different 48-bit round key applies to the plaintext bits to produce a 64-bit output, generated according to a predefined algorithm. The round-key generator generates sixteen 48-bit keys out of a 56-bit cipher key.
- Finally last phase perform Final permutation, reverse operation of initial permutation and the output is 64-bit cipher text.

Step 1: Expansion-The 32-bit bisected-block is expanded to48 bits using the extension permutations, denoted E in the diagram, by duplicating bisect of the bits. The outputs consist of eight 6-bits (8*6=48 bits) piece, each containing a copy of 4 parallel inputs bits, plus a copy of the directly contiguous bit from each of the input pieces to either another side.
Step 2: Key mixing-The result is combined with a subkey using an XOR operation.16 to 48-bit subkey one for each round are derived from the main key using the key schedule.
Step 3: Substitution-After mixing in the sub key, the block is splited into eight 6-bit pieces before preparing by the S-boxes, or substitution boxes. Each of the eight S-boxes substitutions its six input bits with four outputs bits conferring to a non-linear transformation, provided in the form of a lookup table [6].
Step 4: Permutation-Finally, the 32 outputs from the S-boxes is rearranged according to a fixed permutation, the P-box. This is arranged so that, after permutation, each S-box's outputs bits are spread across 4 different S boxes in the next round.



Block Diagram of Multilevel Decryption
Source of Security in Cloud Computing using Cryptographic Algorithms

❖ **Advanced Encryption Standard (AES):**

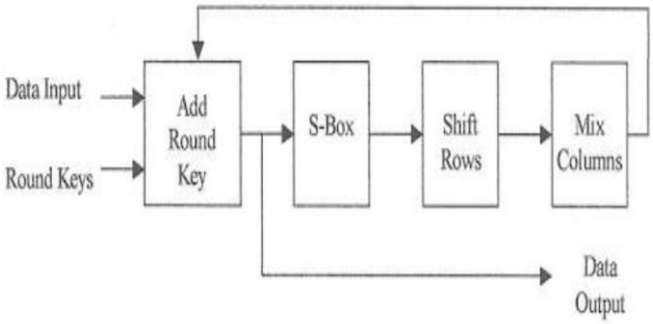
Most adopted symmetric encryption is AES. It operates computation on bytes rather than bits, treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. It operates on entire data block by using substitutions and permutations. The key size used for an AES cipher specifies the number of transformation rounds used in the encryption process [6]. Possible keys and number of rounds are as following:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Step 1: Byte substitution-Substituting each byte of a 128-bit block according to a substitution table. This is a straight diffusion operation.
Step 2: Shift row-A transposition step. For 128 and 192-bit block sizes, row n is altered left round (n-1)0 bytes; row 2 is altered 1 byte and rows 3and 4 are altered 3 and 4 bytes, appropriately[6].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

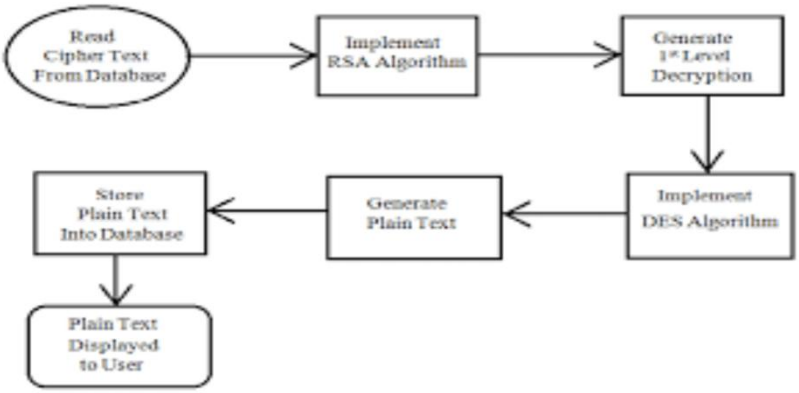
Step 3: Mix column-This step involves shifting left and exclusively-OR bits with themselves. These operations provide both confusion and diffusion.
Step 4: Add subkeys- Here, a segment of the key accurate to this cycle is exclusive-OR with the cycle result. This operation contributes agitation and incorporate the key.



❖ **Rivest-Shamir-Adleman (RSA):**

RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977 [7]. It is most popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and decryption. On the other hand if large p and q lengths are select then it consume more time and the performance gets degrade in comparison with DES [6].

Step 1: Select primes: p=17 &q=11
Step 2: Compute $n = pq$ =17×11=187
Step 3: Compute ø(n)=(p–1)(q-1)=16×10=160
Step 4: Select e:gcd(e,160)=1; choose e=7
Step 5: Determine d: de=1 mod 160 and d < 160 Value is d=23 since
23×7=161=10×160+1
Step 6: Publish public key KU={7,187}
Step 7: Keep secret private key KR={23,17,11}



Block Diagram of Multilevel Encryption
Source of Security in Cloud Computing using Cryptographic Algorithms

❖ **Elliptic Curve Cryptography (ECC):**

Elliptical curve cryptography (ECC) is one of the public key encryption technique that generates best cryptographic keys according to the elliptic curve theory. It creates smaller keys within a short period. Rather than using large prime numbers for key generation, ECC uses the properties of elliptic curves to generate keys. Elliptic curve is a nonsingular cubic curve with two variables in a certain field and an infinite rational point . Each user generates a public-private key pair, where the public key is applied for encryption and signature verification and the private key is applied for decryption and signature generation [1] . The high level of security can be achieved in ECC using a 164 bit key, where the traditional techniques need 1024 bit key [3]. ECC is widely used because of its low computing complexity and better utilization of batter power. Security is attractive feature of elliptic curve cryptography.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

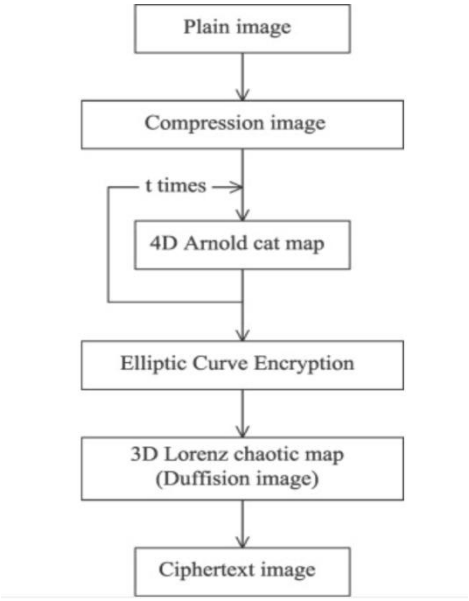
Step 1: The sender and receiver selects two integers *Pri A, Pri B* as private keys.
Step 2: The public keys of both sender and receiver are generated by multiplying the base point *B* of the elliptic curve with the corresponding private keys.

- Public key of sender: $PubA = PriA \times B$;
- Public key of receiver: $PubB = PriB \times B$.

Step 3: The security key is generated as follows:

- Secret Key of sender: $SK = PriA \times PubB$;
- Secret Key of receiver: $SK = PrivteB \times PublicA$.

Step 4: The signature is generated using the hash functions.
Step 5: The signature is sent to the receiver for authentication.
Step 6: At the encryption phase, the message is converted into cipher text using the public keys and a point on the curve.
Step 7: The cipher text is decrypted at the receiver end using the private key.
Step 8: The signature is validated, if the sender's public key is encoded in it.



CONCLUSION

Cloud Computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges are still existing in this technology. Security is the most challenging issue in this technology. Here we conclude that RSA,DES,AES and ECC algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. RSA is comparatively a good technique as it takes much lesser time and more secure because of its asymmetric nature. In this paper, we have suggested a solution that allows storage of data in an open cloud. Data security is provided by implementing our algorithm. Only the authorized user can access the data.

REFERENCES

1. Athena, J. and Sumathy, V. (2017) , Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing. Circuits and Systems Scientific Research Publishing.
2. Pooja Bindlish. *(2016)*, Study of RSA, DES and Cloud Computing, International Journal of Advanced Research in Computer Science.
3. Nidal Hassan Hussein Ahmed Khalid , Khalid Khanfar *(2016)*, A Survey of Cryptography Cloud Storage Techniques , International Journal of Computer Science & Mobile Computing.
4. Shakeba S. Khanand , Prof.R.R. Tuteja. *(*2015) , Security in Cloud Computing using Cryptographic Algorithm, International Journal of Innovative Research in Computer and Communication Engineering.
5. Zaid Kartit , Mohamed El Marraki. (2015), Applying Encryption Algorithm to Enhance Data Security in Cloud Storage , Advance online publication.
6. Nasarul Islam.K.V, Mohamed Riyas.K.V.(2017) , Analysis of Various Encryption Algorithms in Cloud Computing , International Journal of Computer Science and Mobile Computing.
7. Parsi Kalpana, Sudha Singaraju. (2012) , Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication technology.
8. Radhika Patwari, Sarita Choudhary. (2015), Security issues and Cryptographic techniques in Cloud Computing, International Journal of Innovative Computer Science & Engineering.