**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 9, No. 4, August 2019, pp. 2578~2584
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp2578-2584 

# Hybrid cryptography security in public cloud using TwoFish and ECC algorithm

**Siva Sankaran P, Kirubanand V B**
Department of Computer Science, Christ (Deemed to be University), India

**Article Info**

***Article history:***

Received Dec 2, 2018
Revised Jan 1, 2019
Accepted Mar 10, 2019

***Keywords:***

Cloud computing
Cryptography
Elliptic curve Cryptography
Private key
Public key
TwoFish

**ABSTRACT**

Cloud computing is a structure for rendering service to the user for free or paid basis through internet facility where we can access to a bulk of shared resources which results in saving managing cost and time for large companies, The data which are stored in the data center may incur various security, damage and threat issues which may result in data leakage, insecure interface and inside attacks. This paper will demonstrate the implementation of hybrid cryptography security in public cloud by a combination of Elliptical Curve Cryptography and TwoFish algorithm, which provides an innovative solution to enhance the security features of the cloud so that we can improve the service thus results in increasing the trust overthe technology.



***Corresponding Author:***

Siva Sankaran P,
Department of Computer Science,
Christ (Deemed to be University),
Bangalore, 560029-India.
Email: sivasankarangp@gmail.com

## 1. INTRODUCTION

### a. Cloud Computing

Cloud Computing is a distributed architecture and provides a centralized server storage platform to deliver on-demand computing data and services. Cloud Service Provider which offer cloud platform to provide the client to access and use, create their web services, same as like ISP which provides offers to customers and internet facility. Cloud computing is the practice of using remote servers network connected to the internet to store, manage and process data with minimal management effort. The basic mechanism of cloud storage contains four layers: Storage layer, Basic Management layer, Application interface layer and Access layer.

The Storage layer which is responsible for storage of the data, Management layer which ensures security and stability, application interface layer provides an application service platform and the access layer provides the access platform. Cloud providers offer 3 types of services they are Software as a Service, Platform as a Service and Infrastructure as a Service [1].

### b. Symmetric cryptography

The algorithm which use the unique cryptic key for encryption and decryption is asymmetric cryptography. The key is the shared secret between the parties to maintain the secret information. In order to access the information, both the parties will require the secret key which is one of the drawbacks of the private encryption method.

**c. Asymmetric cryptography**

The algorithm where key comes in a pair is a form of Asymmetric encryption, where one is used to encrypt and other to decrypt, It is known as public key cryptography since users create a matching key pair and make one key secret and keeping the other key public. The sender will be able to send the message by encrypting with the help of receiver public key, so only the authorized receiver will be able to decrypt the message because only that user has authorization to access the required secret key.

## 2. LITERATURE REVIEW

Cloud Computing security is a major aspect of the information system, various researches had been made around the world to improve the security in the cloud infrastructure and environment. Rong et al. [2] had mentioned that though several technological methods devote to better security performances in the cloud system, still there are no perfect solutions, and several problems exist. Subasree [3] mentions there are several security threats in the network were network is an interconnected node. In order to maintain the level of security in the network there is three major security principle to be taken into consideration they are 1) Confidentiality 2) Authentication 3) Integrity which requires certain security algorithm such as ECC and RSA. They are designed for providing improved security by the integrity of both symmetric and asymmetric cryptographic techniques. Wang Tianfu [4] explains that the most unsafe method of communication is the internet due to the public network.

Currently, various algorithm techniques are been used to provide protection to information, so in order to improve the security hybrid model is introduced a combination of AES and DES was a significant result has been observed from the proposed solution. Maitri [5] explore that implementation of a single algorithm for security is not efficient for today's world. The proposed system uses AES, Blowfish RC6 algorithm to give block-wise security to the data file. The different algorithm is used to encrypt each and every part of the data. The concept of multithreading technique is used to encrypt all part of the file. Cloud owner upload the files to the cloud server. The file is separated into 8 parts and each part is encrypted simultaneously and the data is stored on the cloud server. When cloud user requests a file they get a stego image using an ID which contains the key information, the process is reversed to decode the file. In hybrid algorithm three keys are used one for data upload on the cloud, the mandatory keys are RSA and AES. They are necessary to download the file from the cloud server.

Bhandari et al. [6] have proposed the important issues in data security and privacy of data. Hybrid encryption is implemented by RSA with AES to improve the efficiency of the security. The RSA algorithm complexity is dependent on how large exponent, symmetric cipher has complexity O(1), it consumes less time when compared to RSA because it needs to store the computations. So the proposed algorithm works better.

## 3. OVERVIEW OF ALGORITHM

The cryptographic algorithm is analyzed to observe the performance evaluation. An algorithm is a step of procedures to solve the problems which obtain the desired output for a given input in a finite amount of time. In this paper we are taking four encryption algorithm and making a comparative study to find which is best to provide security to the cloud, the encryption algorithm includes TWOFISH, DES, RSA, and ECC [7].

### 3.1. Data encryption standard

DES - data encryption standard was first developed by the IBM labs. It contains 56 bits key for the process of encryption and decryption of data, The 16 round of encryption on every 64 bits block of data is required to encrypt the data. It was accepted by the NIST in 1978. It follows a symmetric encryption system which uses a 64-bits block. It has 56 bits key length which makes the algorithm more effective. DES is completely based on the Feistel Cipher. Round function, Key schedule, Initial, and final permutation are required to specify DES.

### 3.2. RSA (rivest-shamir-adleman)

RSA is an asymmetric algorithm where keys typically 1024 or 2048 bits long, the basic concept of RSA is on the fact that it is tough and challenging to factorize a large integer. The algorithm is designed in the way that it consists of two number where one of the numbers is a product of two big prime numbers and from this two prime number the private key is also derived, so in case if anyone can factorize the number, the private key will be compromised. The strength of encryption lies on the key length, if we increase the length or size of the key then the level of encryption will also gradually increase [8].

### 3.3. TwoFish

An efficient symmetric algorithm for data encryption is TwoFish and it is recommended as AES. The design criteria as shown in Figure 1 by NIST requirement standard of AES as follows:

Step 1: Symmetric cipher block of 128-bit
Step 2: Contains no weak keys
Step 3: Simpler design to facilitate the process of implementation and analysis of the algorithm.
Step 4: Flexible design
Step 5: Ability to take key length up to 256 bit.

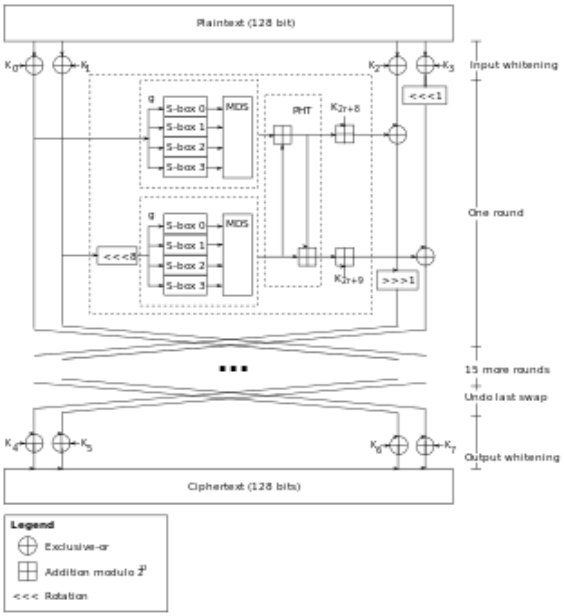


Figure 1. TwoFish algorithm block diagram

### 3.4. Elliptic curve cryptography (ECC)

ECC is a Public-key cryptography which depends on the algebraic structure of elliptic curve over a finite fields as shown in Figure 2. One of the important features of ECC is it requires a small key when compared to another non-ECC algorithm which provides the same level of security. It can be applicable for key agreement, digital signature, pseudo-random generators. ECC has some primary benefits like smaller key size, reduced storage, and transmission requirement, this proves that ECC can provide a similar level of security which other RSA related system with a big module and correspondingly bigger key. ECC can provide security with a 256-bit EC public key which can give a comparable security to a 3072-bit RSA public key [7].

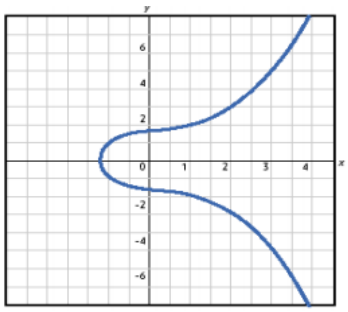


Figure 2. ECC algorithm block diagram

## 4. PROPOSED MODEL

Hybrid Cryptography encryption is an integrated approach of two Encryption Algorithm in order to provide security to data in a public cloud, In this paper Symmetric and Asymmetric type encryption technique are implemented to get an efficient result. This type of cryptography is safe, but they also contain certain drawbacks such as slow in encryption and decryption for a large set of data. The proposed methodology as shown in Figure 3 works in such a way that it integrates the speed of one key encryption and decryption in company with the security that both Public and Private Key provides, which in turn results in a favorably secure type of encryption.

Hybrid Cryptography performs by encrypting the data with a Symmetric Key (Public Key) which will be then encrypted with an Asymmetric Key (Private Key) of the sender. In order to decode the encrypted data, the receiver should first decrypt the public key with the provided Asymmetric Key and then use the Public Key to decrypt the data which is been received. This methodology can be well understood with an example [9].

### 4.1. Steps involved in encryption

i) The first step to be followed is to obtain the user 'X' public key.
ii) Then generate a new symmetric key and encrypt the data using the key.
iii) Now encrypt the symmetric key using user 'X' public key.
iv) Send these two encryption files to user 'X'.

### 4.2 Steps involved in decryption

In Order to decrypt the hybrid ciphertext, the receiver does the following:

i) The receiver needs the key (Private Key) in order to decrypt the symmetric key.
ii) Then the receiver uses the decrypted symmetric key in order to decrypt the original data.

### 4.3. Block diagram

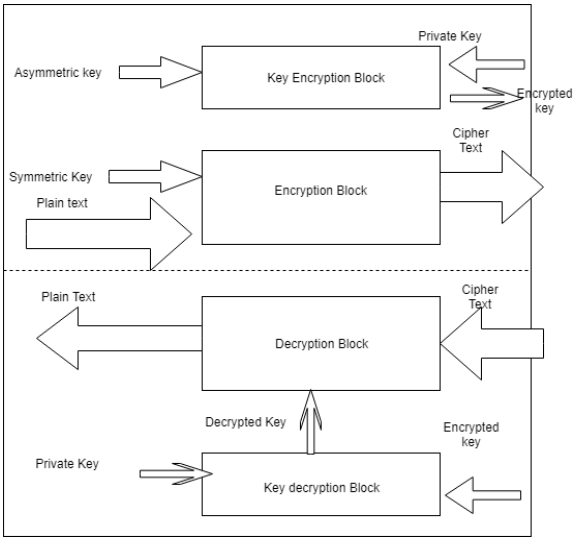


Figure 3. Proposed system block diagram

## 5. RESULT AND DISCUSSION

### 5.1. ECC

The implementation of ECC undergoes three phases where it is integrated with ECDSA as shown in Figure 4 they are: i) ECDSA key generation; ii) ECDSA signature; iii) ECDSA signature verification. The Elliptic curve Digital Signature Algorithm is implemented on EC P-192 in Java language.

#### 5.1.1. Key generation of ECDSA

The EC parameters are (n,P,d,Q,h). The entity A undergoes the following process:

Step 1 : First is to select a EC 'E' as defined on **F2m**. Note that the no of points in E**(F2m)** has to be divisible by a greater prime number n.

Step 2 : now select a point P (summantion) E**(F2m)** of order n.
Step 3 : Statistically same and unpredictable integer 'd' in the interval [1, n-1]
Step 4 : now compute (Q = dp)
Step 5 : The private and Public key of 'A' are d and (E,P,n,Q).

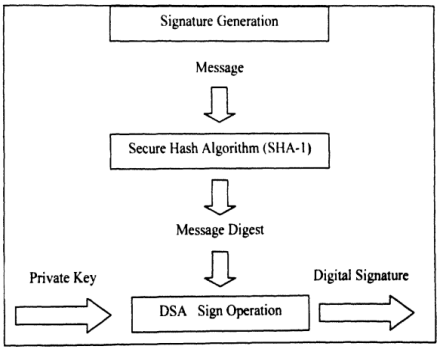


Figure 4. ECDSA key generation block diagram

**5.1.2. Signature generation of ECDSA**

In order the message A to be signed, X need to do the following:

Step 1 : Initially a statistically same and undeterminable integer y is selected in the interval between [1, n-1].
Step 2 : Then we need to compute yP=(x,y) and r=x mod n. If r=0 then proceed to first step.
Step 3 : y-1 mod n is computed.
Step 4 : s=y-1{h(m)+dr} mod n is computed, where in this equation h is the secure Hash Algorithm (SHA-1).
Step 5 : Go to step 1 if s=0.
Step 6 : The integers pair (r,s) for the message A is the signature.

**5.1.3. Signature verification of ECDSA**

In Order to verify X's signature (r,s) on m. Y does the following as shown in Figure 5:

Step 1 : First step is to get the authentic of X's public key (E,P,n,Q). Then verify that r and s are integers in the interval [1, n-1].
Step 2 : Then compute w=s-1 mod n and h(m)
Step 3 : Compute u1= h(m) w mod n and u2= rw mod n and then compute u1p+u2Q= (X0, Y0) and v=x0mod n.
Step 4 : If v=r then accept the signature.

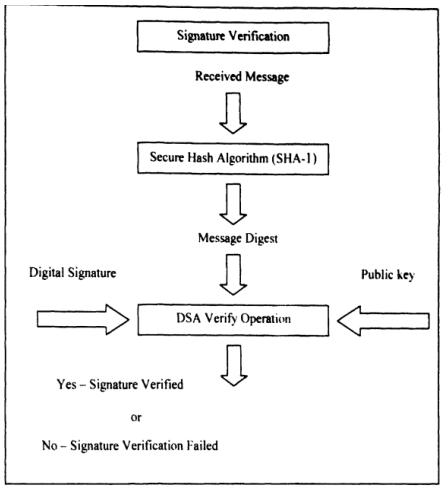


Figure 5. ECDSA signature verification block diagram

### 5.2. TwoFish

There are several things which to be considered when implementing a TwoFish algorithm which is as follows:

Step 1 : The 128 bits input is divided into four parts, 32 bits each are using little-endian convention. Right part contains two part and the left part contain the remaining two.

Step 2 : R0,1=P⊕Ki; i=0,.....,3 Bit-XOR input in advance with the four key parts. K is the key, Ki means the sub key [10].

Step 3 : Feistel network structure is used in the Twofish algorithm and it consists of 16 iterations. Twofish Function f consists of many stages:

a. The Function g, which contains four s-box and MDS matrix
b. pseudo-Hadamard transform
c. IPM addition of the key result

### 5.3. Comparative study

A comparative study on different algorithm as shown in Table 1.

Table 1. A comparative study on different algorithm

| ALGORITHM | DES | RSA | ECC | TWOFISH |
|---|---|---|---|---|
| ROUNDS | 16 | 1 | 1 | 16 |
| BLOCK SIZE (Bits) | 64 | Variable block size | Stream size is variable | 128 |
| SECURITY LEVEL | Satisfactory | Good | Highly secure | Secure |
| SPEED | Very slow | Average | Very Fast | Fast |
| KEY LENGTH (Bits) | 64 | Key length depends on number of bits | Small but effective | 128,192,256 |
| ATTACK ROUND | Exclusive key search, Differential analysis | Brute force, timing attack | Doubling attack | Differential attack, related key attack |

## 6. IMPLEMENTATION

In order to implement the proposed model we used java language, The Java source code works effectively and outcome contains no error. Following this screenshots are attached which shows the output of the java implementation as shown in Figure 6.

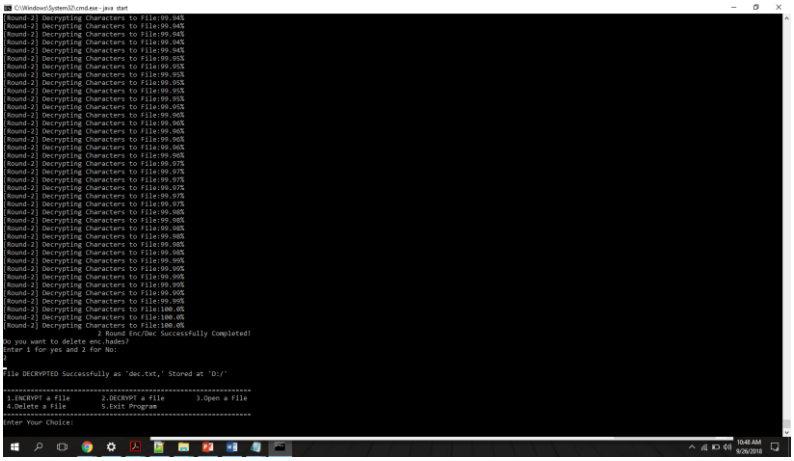

Figure 6. Java implementation of algorithm

## 7. CONCLUSION

This Proposed work concludes that the solution provided by the hybrid encryption using ECC and Twofish provides a better solution when compared to other encryption algorithms. This solution can be applied in real time cloud platform to provide a better security to the data. In future, this method of encryption can be used in local area networks to enhance the security and prevent from any cyber attacks.

## REFERENCES


[1] S. Choudhury, "Data encryption in public cloud using multi-phase encryption model," *International Journal of Engineering & Technology*, vol/issue: 7(1), pp. 223-227, 2018.

[2] *Rong, C., Nguyen, S. T.,* & Jaatun, M. G. (2013, May). *Beyond lightning: A survey on security challenges in cloud computing*. *Computers & Electrical Engineering*, 39(1), 47–54. doi:10.1016/*j*.compeleceng.2012.04.015 Ryan M. D. (2013).

[3] S. Subasree, "Design of A New Security Protocol Using Hybrid Cryptography Algorithms."

[4] W. Tianfu, "Design of a Hybrid Cryptographic Algorithm," *International Journal of Computer Science & Communication Networks*, vol/issue: 2(2), pp. 277-283.

[5] P. V. Maitri, "File storage in Cloud Computing using Hybrid Cryptography Algorithm," *IEEE*, pp. 603-610, 2016.

[6] A. Bhandari, "Secure algorithm for cloud computing and its applications," *IEEE*, pp. 188-192, 2016.

[7] K. Singh, "Implementation of Elliptic curve Digital Signature Algorithm," *International Journal of Computer Application IJDCST@June-July-2015, Issue-V-3, I-5, SW-23*.

[8] Dr. K.L. Vasundhara *et.al. Int. Journal of Engineering Research and Application www.ijera.comISSN: 2248-9622, Vol. 8, Issue 1, (Part -I) January 2018, pp.49-52

[9] A. Puri, "Enhancing Cloud Security by Hybrid Encryption Scheme," *International Journal of Advance Engineering Technology E-ISSN 0976-3945*.

[10] G. K. Kumar, "Comparative study on Blowfish and Twofish Algorithm for Cloud security," *International Journal of Current Trends in Engineering and Research*, e-ISSN 2455–1392 Volume 3 Issue 9, September 2017pp. 1–11.


## BIOGRAPHIES OF AUTHORS

Siva Sankaran P, Research Scholar, , Department of Computer Science,, Christ( Deemed to be University), Bangalore – 29.

Dr. Kirubanand V B., Associate Professor, Department of Computer Science, Christ( Deemed to be University), Bangalore – 29.