ECC and MAES based Data Secure Mechanism for Cloud Computing

Stephy Patel[1], Nirav Shah[2]
[1]*M.E. Department of Computer Engineering, Silver Oak College of Engineering and Technology*
[2]*Department of Information Technology, Silver Oak College of Engineering and Technology*

Abstract **- With the advancement in information technology, everyone moves towards pleasure, ease, and luxury. From which the most advanced and usable field is Cloud Computing which uses the internet and gives access to storing the data to the user. With the rapid increase in the number of users, there is a rise in issues related to hardware failure, web hosting, space, and memory allocation of data, which is directly or indirectly leading to the loss of data. With the objective of providing services that are reliable, fast, and low in cost, we turn to cloud-computing practices. In these paper sheds light over the security issues and challenge. In cloud computing and puts emphasis on cloud computing service types and the different types of delivery along with their security challenges and threats. A probabilistic method to encrypt the information using AES. At AES algorithm is not only for protection it can be also used in huge speed. AES provides well-built security from third party. In this proposed work, we implemented a hybrid approach in which we apply the MAES and ECC method for data protection and Robustness for cloud and also provides protection for the information, from the illegal abuser and its offers probity to the client.**

Index Terms **- Cloud Computing, AES algorithm, ECC, MAES, robustness.**

1.INTRODUCTION

Cloud Computing is a gathering of coordinated network, hardware, software, and internet. Cloud Computing enables on-demand access to several computing resources in a pay-per-use manner [6]. Cloud Platform provides on demand services which are always on anywhere, anytime, and anyplace. Cloud Computing is an information technology paradigm that provides ubiquitous access to shared, centralized pool of services which includes servers, computer networks, data storage, applications, and various other services over the internet [4]. It enables on- demand rationing, scalable and elastic computing, storage, and network resources. In figure also contains mobile's applications which are stored on database server, and you can used anywhere. Cloud computing is typically described in one among two ways. Either supported the deployment model, or on the service that the cloud is offering. Based on a deployment model, we will classify cloud as: public, private, hybrid, community cloud.

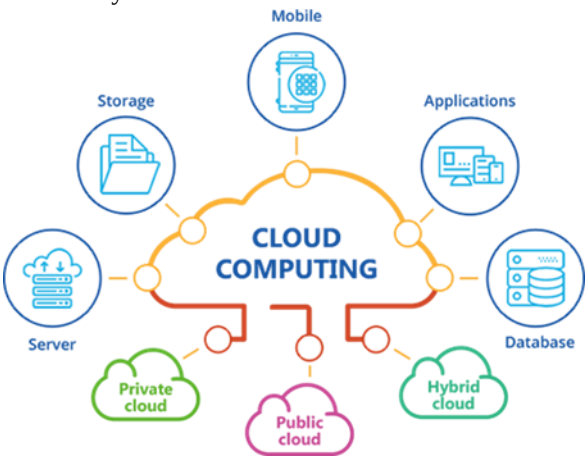

Fig. cloud computing overview

1.1 Services in cloud computing

Cloud services are usually divided within the three main types, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

a. Software as a Service (SaaS)

In this, the administration of these services such as updating, and patching are in the provider's responsibility. The one big advantage of SaaS is that each one client is running an equivalent software version and new functionality are often easily integrated by the provider and is therefore available to all the clients. E.g., Salseforce.com.

b. Platform as a Service (PaaS)

PaaS Cloud providers offer an application platform as a service, E.g., Google App Engine. This enables clients to use custom software using the tools and programming languages offered by the provider. The Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

c. Infrastructure as a Service (IaaS)

IaaS delivers hardware resources like CPU, network or disc space components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and may be accessed across the web by the client. The clients have full control of the virtualized platform and are not responsible for managing the underlying infrastructure.

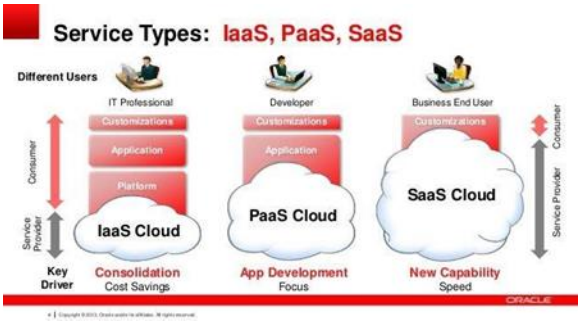

Fig. service of cloud computing

2.PROBLEM DEFINITION

As per survey is based paper securing data and reducing the time traffic using AES encryption with dual cloud certain limitations in existing systems like robustness, security, privacy of data, speed and also time complexity.

3.BACKGROUND

3.1 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) algorithm not only for security but also great speed. AES is the current standard for secret key encryption. AES is a symmetric key algorithm. It is having various chippers with different keys and the block size. In this plaintext is encrypted with the help of AES and then the ciphertext which we have got will again encrypt likewise there will be various round like the AES algorithm includes 10, 12 and 14 round with 128, 192, and 256 key bits. As there are various rounds in this algorithm the plaintext is encrypted many times and this helps the data to have the security [3].

Encryption works by taking plain text and converting it into cipher text, which is made up of seemingly random characters. Only those who have the special key can decrypt it. AES uses symmetric key encryption, which involves the use of only one secret key to cipher and decipher information.

128-bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on a cloud. The proposed model uses Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.

3.2 Modified Encryption Standard (MAES)

Advanced Encryption Standard (AES) is a well-known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. modification to the Advanced Encryption Standard (MAES) to reflect a high-level security and better image encryption. The modification is done by adjusting the ShiftRow phase. Modify the AES to be more efficient and secure way by adjusting the ShiftRow phase [4].

The modified AES (advance encryption standard) ciphers as it can encrypt 128-bit data blocks within 1000 cycles with low power, time, and delay of network consumption. The other work of the frameworks is load balancing, trust, and resource management on the network efficiently.

3.3 Elliptic curve cryptography (ECC)

ECC is a public key cryptography which has public and private keys for authentication. The utilization of elliptic curves in cryptography. ECC is known as a sort of PKC which is built upon algebraic structure of elliptic curve over finite fields [5].

Elliptic curve cryptography (ECC) is a public key encryption technique based on an elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

ECC can achieve the same level of security with a 164-bit key that other systems require a 1,024-bit key. Because ECC helps to establish equivalent security with lower computing power and battery resource

usage, it is becoming widely used for mobile applications.

4.LITERATURE REVIEW

In this paper [8], Cloud computing has considerably impacted every division of our life and commerce structures. We have some advance encryption system. For superior information security and confidentiality, we have AES 256, IDA and SHA 512. In the process of indoctrination, the unusual data encrypted by AES 256 algorithm. The transformed file is supported into several divisions. While decoding authentication are observed. Next, recreate the encrypted information by IDA, after decrypting unusual data by AES 256 to acquire unusual information.

On output, execution time lag in decoding process. Encoding outcome depends on the value (p, q). When the threshold is big, the confirmation time reduced and reform time increase. The threshold is tiny, the confirmation time raise and reform time reduce. In cloud computing we have some security issues like dishonest access and change of information. Numerous amounts of cloud users used to launch the data in the cloud. Storing data in the cloud can be quickly recovered. Data security will be measured by software engineer on the proposed area in cloud storage. Pay concentration to inform redundancy and security.

The redundancy is to secure information and isolation to guarantee inter-information independence. There are two threats arise in information security in the cloud are information storage and transmission. Discretion and reliability of information are foundation of data protection. the Information security technique of relief and transit may differ.

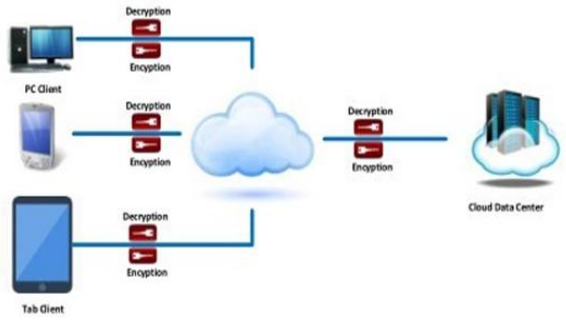

Fig. encryption and decryption

Initially, Heroku requires few applications to protect the information prior to storing it in the database. The leading and secured encryption algorithm is AES.

AES (Advanced Encryption Standard) is a symmetric-key block chipper with block size difference of 8 to 32 bytes. In this Proposed work, we talk about securing information and reducing the time traffic using dual cloud in AES encryption. We execute Heroku cloud as platform as a services, then we employ AES in the webpage to secure information.

We are using the dual cloud for data storage and efficient retrieval. Redundancy is a simple way to protect the data privacy. Then, the separation is the result of particular customer information is saved on the same cloud platform, so it guarantees the inter data independence.

5.PROPOSED MODEL

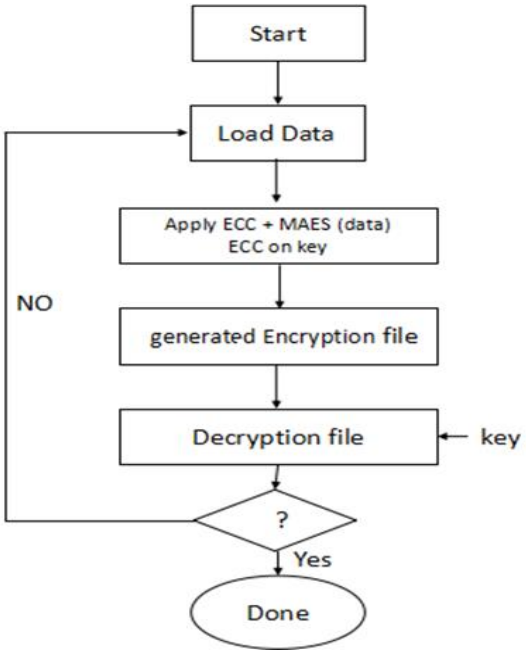

Fig. proposed model

Steps of the proposed system:

1. Start
2. Load the data from different server
3. Apply ECC and MAES algorithm
4. Output of hybrid algorithm will be encrypted file
5. If file can be decrypted on the key
6. Then decrypted file is successful
7. Otherwise reload the data
8. stop

ECC Algorithm:

elliptic-curve based public-key encryption / decryption (asymmetric encryption scheme based on

ECC). This is non-trivial and usually involves a design of hybrid encryption scheme, involving ECC cryptography, ECDH key exchange and symmetric encryption algorithm. The elliptic curve cryptography (ECC) does not directly provide encryption method. Instead, we can design a hybrid encryption scheme by using the ECDH (Elliptic Curve Diffie–Hellman) key exchange scheme to derive a shared secret key for symmetric data encryption and decryption.

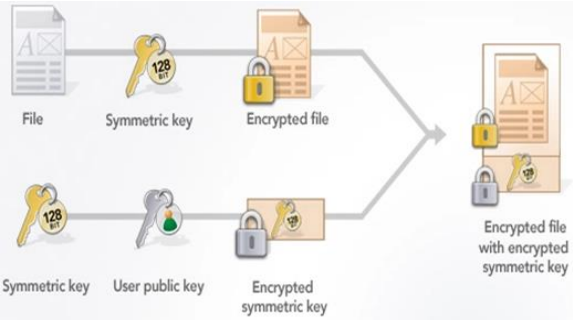

Fig. hybrid encryption schema (the encryption process)

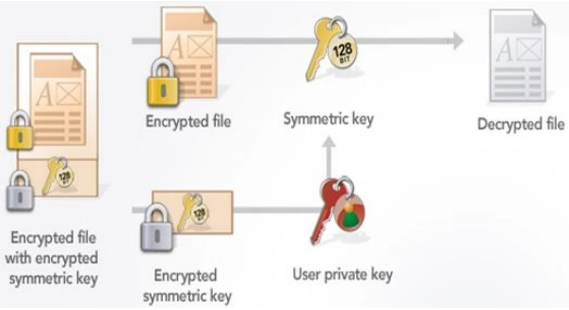

Fig. hybrid decryption schema (the decryption process)

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -Elliptic Curve

P -Point on the curve

n -Maximum limit (This should be a prime number)

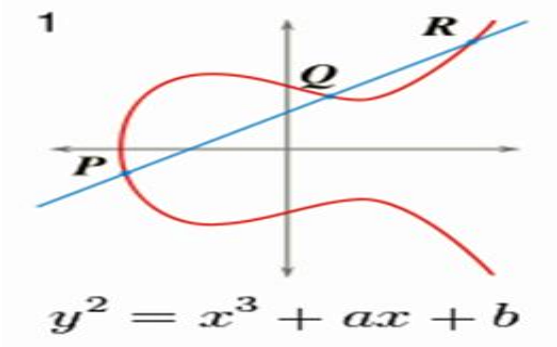

Fig. ecc

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number 'd' within the range of 'n'.

Using the following equation, we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.

'Q' is the public key and 'd' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

Proof

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

MAES Algorithm:

A new modification for the AES algorithm (MAES) is done by replacing the MixColumns stage with random Generated IP vector for Permutation or Transposition stage at every session of encryption. This will increase the speed of the algorithm without a decrease in the security of the AES algorithm. In addition, the security of the MAES algorithm can be enhanced using the permutation stage that changes the IV vectors at every round of the encryption process.

The design of the MAES algorithm will ensure the following:

1. Speed up the encryption and decryption processes by replace MixColumns stage with simple xor operations.
2. The input state will be the first input for the xor operation.
3. Increase the decryption level of complexity by
   a. Using random number generator output as second input for xor operation.
   b. Key dependent random number generator.

Algorithm:

```
ShiftRows (byte state [4, Nb] )
begin byte t[Nb]
if state[0][0] odd numbers
for r = 1 step 1, 3
x = r mod 4
if x = 0 step 0 to x + 1
for c = 0 step 1 to Nb – 1
t[c] = state[r, (c + x) mod Nb]
end for
for c = 0 step 1 to Nb – 1
state[r,c] = t[c]
end for
end for
else
for r = 2 step 2, 4
k = 0
x = r mod 4
if x = 0 step 0 to 3
for c = Nb - 1, c >= 0, c -1
t[c] = state[x, (c + x) mod Nb , k + 1
end for
for c = 0, c < Nb , c 1 +
state[x,c] = t[c]
end for
end for
End
```

6.CONCLUSION

The combination of ECC & MAES gives best security for Data Migration in cloud computing. As this is a combination of Symmetric and Asymmetric key algorithms which provides strong security to any robust system. Benefit of using ECC is that it uses smaller key for the same level of security with very fast key generation, and it also provides fast encryption and decryption, whereas MAES is used for strongly secure transmission of data. Modification of AES makes it more efficient and secure by doing Shift row operation which will be quick than AES. So, after working on proposed model approach, will we get 15.8 sec time complexity in MATLAB.

REFERENCES

[1] Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, IEEE 2013.

[2] Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi, “Data Security in Cloud Computing Using AES Under HEROKU Cloud”, IEEE, 2018.

[3] Abdulkarim Amer Shtewi†, Bahaa Eldin M. Hasan, Abd El Fatah.A. Hegazy, “An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems” International journal of computer science.

[4] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, Zurina Mohd Hanapi, “Comparison of ECC and RSA Algorithm in Resource Constrained Devices”, IEEE.

[5] Wu Feng Sheng, “Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm”, IEEE, 2018.

[6] Poorvika singh negi, Aditya Garg,” Intrusion Detection and Prevention using Honeypot Network for Cloud Security”, IEEE,2020.

[7] Abhinav Varma, Komal Saxena, Sunil Kumar Khatr,” PREVENTIVE MEASURES TO SECURE ISSUES IN CLOUD COMPUTING,” IEEE,2019.

[8] R.Jayaraj, M. NandhaKumar, A.Sakthi Kumaran,” Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud”,IEEE,2019.

[9] Syed Rizwan, Muhammad Zubair,” Basic Security Challenges in Cloud Computing”, IEEE,2019.

[10] T.Ramaporkalai ”security algorithm in cloud computing”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 2017.