ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6667–6678
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.24 Spec. Issue on CAMM-2020

DUAL ENCRYPTION MODEL FOR PRESERVING PRIVACY IN CLOUD COMPUTING

OM PRAKASH JENA[1], ALAKANANDA TRIPATHY[2], SAMBIT SWAGATAM[3], SMITA RATH[4], AND ALOK RANJAN TRIPATHY[5]

ABSTRACT. Secure data transmission is an essential prerequisite of every cloud-based structures. Various networks such as e-commerce, online banking and even software applications operate with cloud infrastructure and transfer the tremendous amount of crucial data daily. Fundamentally, this paper deals with risk factors that are security issues faced during cloud data management. This paper addresses a hybrid encryption technique to protect cloud privacy and security. Elliptic Curve Cryptosystem (ECC) and Advanced Encryption Standard (AES) are the two best asymmetric encryption algorithms and symmetric encryption technology, respectively. The AES-ECC hybrid cryptosystem merges the benefits of AES algorithm to speed up data encryption with ECC algorithm based on symmetrical session key exchange. In the proposed method the delay factor is minimized and is computationally efficient, robust and secure.

1. INTRODUCTION

In recent years, computing resources are more affordable, more powerful and more widely available than ever before because of the proliferation and rapid growth of processing and storage technology and the increase on the Internet. Such software advancement is generally referred to as cloud storage. Cloud

[5]*corresponding author*

2010 *Mathematics Subject Classification.* 68W99.

Key words and phrases. AES, ECC, Hybrid Cryptography, Delay Timing.

storage offers a convenient electronic platform that allows an increased workload to be managed without impacting frame execution. Distributed services are spread around the network in a transparent framework of cloud computing. But Cloud servers have plenty of malware or unauthorized users. They still attempt to exploit data or bombard their accounts by registered cloud consumers. So the information in the cloud needs to be protected. Cloud computing has many threats regarding the security of raw data or vital information. All traffic among consumers and service provider networks is stored in a cloud computing environment. If attackers have a connection to the cloud network, they can quickly manipulate and access the data. Cross-data would usually be shared between clients in the same domain. Information from different clients is most probably held in the same cloud. A mechanism for securing consumer information by distinguishing it from others is therefore essential.

The conformity process in the cloud is Complex by the fact that information is stored in the data provider's centres that may provide for administrative compliance issues like confidentiality, security and discrimination which must be done by the provider.

In this paper, we have discussed a dual encryption model to preserve privacy in cloud computing. The proposed model consists of AES and ECC algorithm based encryption method to make the model more robust and secure.

2. Literature Survey

Cloud computing has a significant impact on every segment of our life and business structure. Different authors also looked at various architectures and applications with other systems and different approaches to software design can be implemented in cloud technology. Cloud storage stability is thus the main problem in maintaining our data security.

Amandeep Verma and Sakshi Kaushal et al. [1] investigate about Security concerns for emerging cloud computing systems. Since Cloud Computing refers both to applications provided services over the Internet and to infrastructures (i.e. hardware and network software in data centres) that provide these services, which pose security concerns in terms of various applications and infrastructures, further security concerns, such as availability, confidentiality, honesty protection, authorization and so on, should be taken into account.

Alakananda Tripathy et al. [2] proposed a new hybrid model which results faster encryption of data with less memory for key storage. In their paper ECC is used for sharing key exchange among nodes. The RC4 symmetric key algorithm is used for encryption and decryption. It motivate us to develop a new hybrid cryptographic algorithm.

Snehal Rajput, J.S. Dhobi et al. [3] describes that Cloud infrastructure relies on utility and deploys on-demand infrastructure services. Cloud providers must ensure that all their resources, i.e. infrastructure, network, applications and customer information, are safe. That cloud providers have a proper algorithm that provides data protection in the cloud. This paper presents a study of numerous well-known encryption technique. It makes a comparison among Digital Signature Along with RSA Encryption, DES algorithm, Single Sign-on Algorithm, and elliptical curve cryptography.

Akashdeep Bhardwaj et al. [4] describes the classification of different security algorithm for cloud computing, i.e. many types of encryption algorithms like Diffie - Hellman, AES and RSA. It also discussed about encryption and decryption processes in cryptography. In this article, risks and assaults on cloud data infrastructure will be studied. Cloud computing environment requires different protection mechanism for the provision of protection service such as validation, authorization, data integrity and confidentiality; a part of cryptography also which are described by the author of this paper. Also, this paper mentioned some of the currently used encryption algorithms. Such algorithms focus basically on the different current encryption techniques and the contrast between algorithms.

Vishwanath S Mahalle et al. [5] described a technique for hybrid AES and RSA encryption in which the 128-bit AES secret key and the 1024-bit RSA key are used. They proposed a system that generally comprises of two modules. That is the Upload Module and Download Module. The upload module consists of 4 parts, i.e. authentication, upload, key generation, encryption and similarly, the download element consists of two parts, i.e. decryption and download. In the authentication part, the user gives his identity to the cloud service provider by a unique username and password. In the upload part, the file will be uploaded in a secure path. The key generation part generates the key as its name implies, and finally, the encryption part encodes the file using the hybrid algorithm. Again in the download module, the decryption part returns the plain text file from the

ciphered file, and the download part simply downloads the file for the user. In this system, the data is first stored in a temporary directory. After encrypted by RSA and AES algorithm, it will be stored in the cloud permanently according to the user. In this technique, the user has to enter the AES secret key to store data in the cloud and have to enter the same key to retrieve the data from the cloud. As a result, high security will be provided by the hybrid (AES and RSA) algorithm.

Bih-Hwang Lee et al. [6] studied that the researchers are mixing AES 256 (Advanced Encryption Standard), IDA (Scattering Algorithm of Information) and SHA 512 (Secure Hash Algorithm) to improve data security and privacy. The original data are encrypted with the AES 256 encryption standard throughout process encoding; the encryption produced is randomly generated by the IT manager. This paper takes Heroku cloud as a platform and implements AES on the website to maintain the security of the data. Heroku cloud is PaaS provider which supports Python, Java, PHP, Ruby, go and Scala. It takes PHP installation to run Heroku locally using CLI. AES is not only significant for speed but also provides higher security and one of the most effective algorithm. It also addresses the disadvantages of the AES that is AES can not tolerate the Brute Force attack and Linear Cryptanalysis.

Wu Feng Sheng [7] describes, by performing an ECC algorithm simulation test, an RSA encryption algorithm and a DSA Matlab encryption algorithm conclude that the ECC offers the apparent benefit of resistance against attacks. This is due to the relatively high computational complexity of the ECC algorithm in the discrete logarithm elliptical curve group. DSA encryption algorithms perform equal performance with the 160 bit ECC encryption algorithm and the 1024bit RSA length. RSA security required 1024 bits for corporate use and 2048 bits for precious keys. The advantage of ECC over RSA is therefore apparent as it can deliver the equal level of security having a shorter key length. A secured ECC cryptosystem requires a minimum key size of 160 bits or higher.

Akash Dutta et al. [8] explained that Elliptical curve equations provide a significant encryption functionality or purpose: the operation has simple performance, but the reversal is extremely complex. The problem's complexity lies in the key size of the elliptic curve.

Sandip Dutta et al. [9] proposed that the arrangement of focuses which meet a certain numerical requirement is an elliptical bending. The condition for a

similar elliptical grade bend is in the form: $y^2 = x^3 + ax + b$. ECC uses a minimal encryption key for helping to reveal a disordered text in encrypted computation. This succinct key is quicker than any other open key calculation for indigenous encipher and enables low recording power. Let's say, 160-piece ECC encipher key from a 1024-piece RSA encipher key offers equivalent protection and this to 15 times faster, depending on the platform on which it is being performed.

Neelendra Badal et al. [10] also builds a hybrid encryption standard by taking AES and FHE (Fully Homomorphic Encryption Scheme) and discussed how the hybrid algorithm is better than one single encryption. But there exist some drawbacks of their hybrid system. That encryption speed of the homomorphic algorithm is slow, that takes much time to encrypt a larger file. That's why it is not recommended for a large volume of file and only a single public key is generated by the algorithm which may not protect the data adequately.

3. Proposed Work

The core aim of the paper is based on to protect the valuable data from unauthorized access or malicious activity. Basic AES and ECC are hybridized to improve the level of data security.

3.1. **AES Security Algorithm.** AES is a block cipher designed to substitute DES and 3DES. It does not use a Feistel structure that is it does not use the same algorithm for encryption and decryption. AES Algorithm has four phases:

- Bytes substitution operation
- Shift rows operation
- Mix columns operation
- Add round key

3.2. **ECC Security Algorithm.** In Elliptical Curve Cryptography we use the equation in the form $y^2 = x^3 + ax + b$. This is also called Weierstrass equation, in which a and b are consistent with $4a^2 + 27b^2 \neq 0$. Algorithms for decryption and encryption are based on point multiplication. P is the base point where point multiplication is performed is fixed. Point multiplication is also called scalar multiplication. All ECC operations are carried out in the final stage. The elementary operation over the curve is point doubling and point addition. Also,

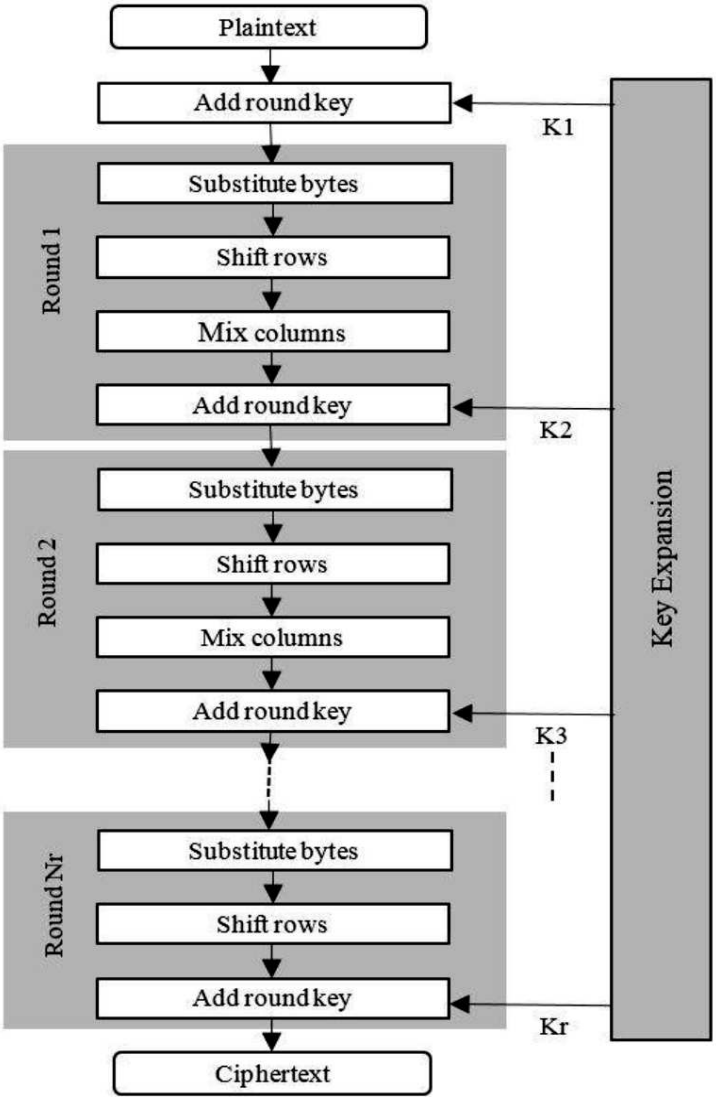

FIGURE 1. Flowchart of AES encryption

point multiplication is the most time-intensive process in addition ECC algorithm.

3.2.1. *Key generation*. The design of the ECC Encryption requires a key generation of both the public key and the private key. The transmitter encrypts the message employing a public key, and the receiver decrypts the message with the help of a private key.

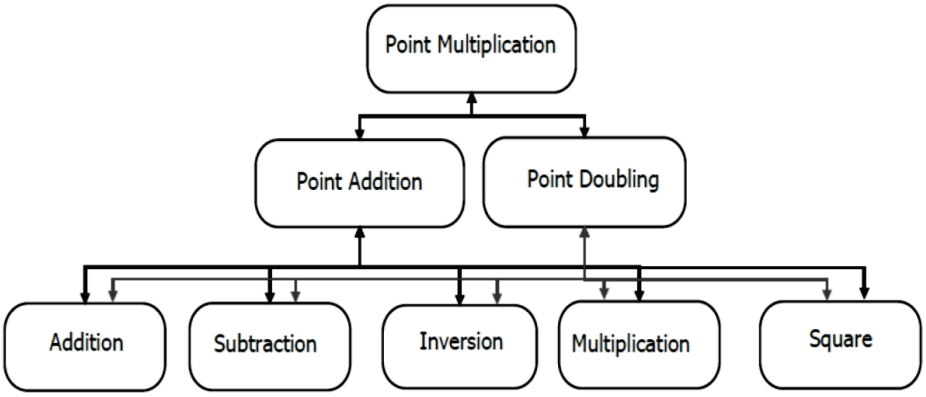

FIGURE 2. Pyramid of Point multiplication

Suppose A and B wants to communicate with each other. Both agree on a common elliptical curve equation and a generator Q.

Let, Private Key of $A = n_A$ $(n_A < n)$ and Private Key of $B = n_B$ $(n_B < n)$. Similarly, Public Key of A, is $P_A = n_A.Q$ and Public Key of B, is $P_B = n_B.Q$

3.2.2. *Encryption.* A want to transfer a secret message P_M to B by using the Public Key of B. The following equation is used for the encryption:

$$C_m = KQP_m + KP_B, \tag{3.1}$$

where K is defined as a random integer with the range 1 to $n - 1$ and C_m is the ciphertext.

A send the message to B. When the encrypted message from A delivers at B, B decrypts the ciphertext into plain text using his or her public key and gets the original message.

$$P_m = P_m + KP_B - n_BKQ. \tag{3.2}$$

3.3. **AES - ECC Hybrid Encryption Architecture.** Figure 3 shows how the AES algorithm encrypts the plain text first, and then the ECC algorithm encrypts the key of AES encryption to ensure maximum protection of data. Thus the medium is insecure; the dual encryption process makes the data transform secure.

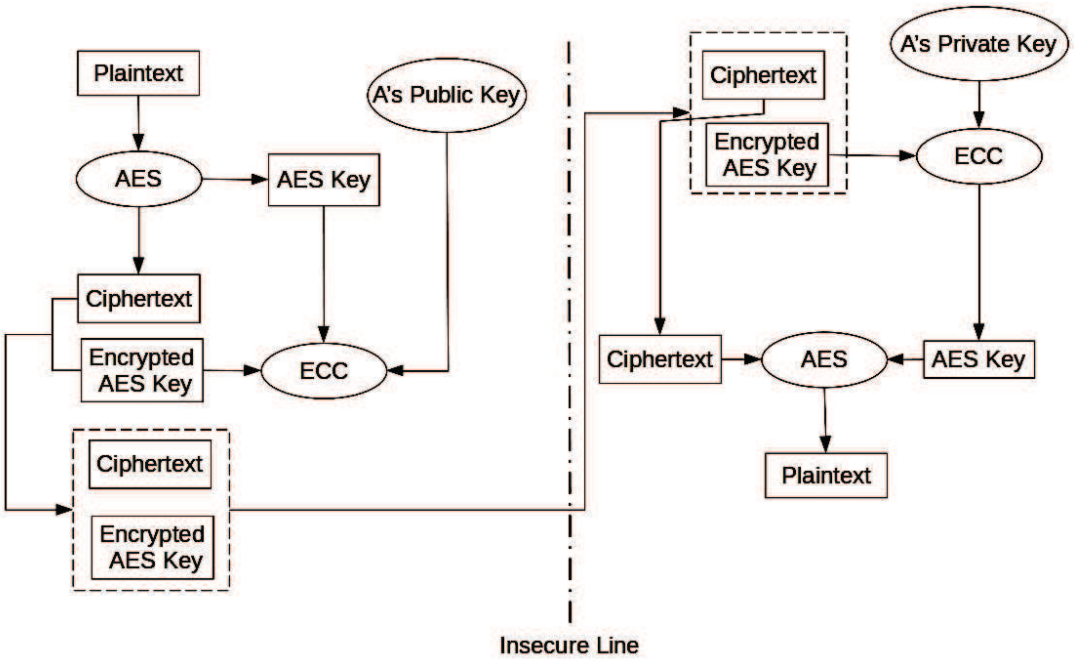

FIGURE 3. Hybrid Cryptosystem

4. RESULT ANALYSIS

Both asymmetric and symmetrical key algorithms are benefiting from the AES-ECC cryptosystem.

4.1. **File Encryption and Decryption.** The plaintex shows in figure 4 in the .txt file which is going to be encrypted by the dual encryption process. Figure 5 is the result after successful encryption which is also in .txt file and is the ciphertext. The file is in encrypted form, which is not readable.

4.2. **Delay Calculation.** The delay calculation will be done by taking the time after the successful run and before reload of the file.

$$Delay\ Calculation = a_T - b_T, \tag{4.1}$$

where a_T = Time after successful load and b_T = Time before load. We have taken different file sizes (in kb) and delay time (in second) for encryption and decryption process. We are considering the comparison between encryption and decryption by the table 1 and figure 6.

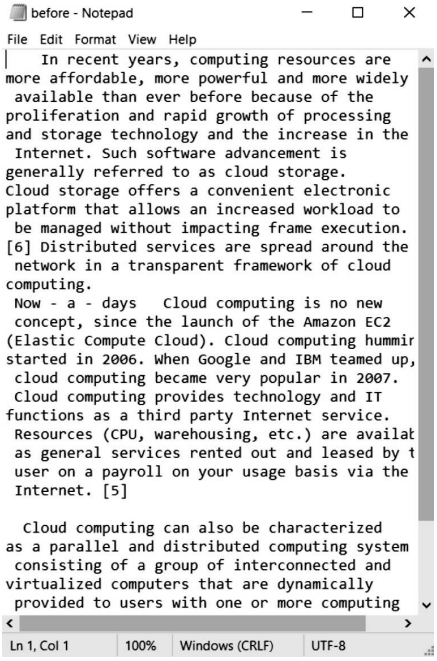

FIGURE 4. Plaintext

FIGURE 5. Ciphertext

TABLE 1. Decryption time of AES and ECC.

File Size (in KB)	Encryption (in Sec)	Decryption (in Sec)
1080	0.5	0.5
1919	0.8	0.8
3200	1.7	1.3
5080	2.4	1.9
19080	5.6	4.9

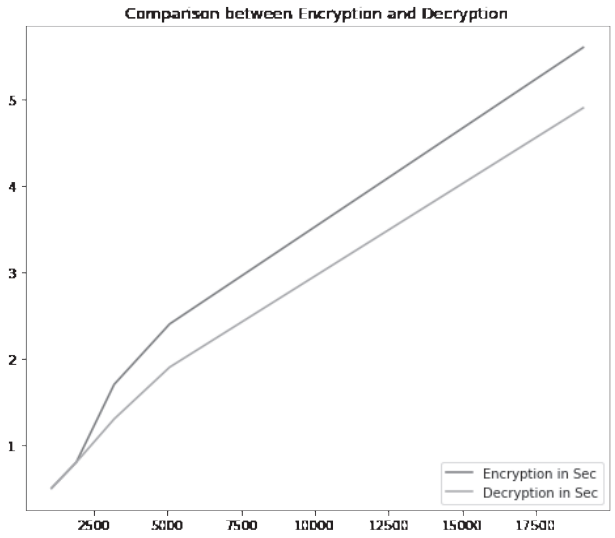

FIGURE 6. Comparison between Encryption and Decryption

5. CONCLUSION

Security and privacy confidentiality is a crucial concern for cloud infrastructure data management. Because the CSP is a non-trusted third party, therefore we can't store raw data without encryption because of confidentiality issues. In the proposed work, a secure data transmission and storage in cloud by the help of hybrid cryptosystem is discussed. The combination of AES and ECC simultaneously to proliferation the integrity and confidentiality of the system, by which we can apply both symmetric and asymmetric encryption to add more protection to the cloud data. Therefore the anticipated model affords a well-organized AES and ECC based encryption method which is more secure, robust and computationally efficient.

REFERENCES

[1] A. VERMA, S. SAKSHI: *Cloud computing security issues and challenges: a survey*, In International Conference on Advances in Computing and Communications, Springer, Berlin, Heidelberg, (2011), 445-454.

[2] A. TRIPATHY, S. KUMAR PRADHAN, A. RANJAN TRIPATHY, A. KUMAR NAYAK.: *A New Hybrid Cryptography Technique in Wireless Sensor Network*, International Journal of Innovative Technology and Exploring Engineering (IJITEE), **8**(10) (2019), 121-131.

[3] S. RAJPUT, J.S. DHOBI, L.J. GADHAVI: *Enhancing data security using aes encryption algorithm in cloud computing*, Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems, **2** (2016), 135-143.

[4] A. BHARDWAJ, G.V.B. SUBRAHMANYAM, V. AVASTHI, H. SASTRY: *Security algorithms for cloud computing*, Procedia Computer Science **85** (2016), 535-542.

[5] V.S. MAHALLE, A.K. SHAHADE: *Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm*, International Conference on Power, Automation and Communication (INPAC) IEEE, (2014), 146-149.

[6] B.-H. LEE, E. KUSUMA DEWI, M. FARID WAJDI: *Data security in cloud computing using AES under HEROKU cloud*, 27th Wireless and Optical Communication Conference (WOCC), IEEE, (2018), 1-5.

[7] F.S. WU: *Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm*, International Conference on Virtual Reality and Intelligent Systems (ICVRIS), IEEE (2018), 125-129.

[8] A. DUA, A. DUTTA: *A Study of Applications Based on Elliptic Curve Cryptography*, 3rd International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, (2019), 249-254.

[9] S. SOM, R. MAJUMDER, S. DUTTA: *Elliptic curve cryptography: A dynamic paradigm*, International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), IEEE, (2017), 427-431.

[10] L. KUMAR, N. BADAL: *A Review on Hybrid Encryption in Cloud Computing*, 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, (2019), 1-6.

[1,3,5]Department of Computer Science, Ravenshaw University, Cuttack-753003, Odisha, India.

E-mail address: [1]jena.omprakash@gmail.com

[2,4]Department of Computer Science & Engineering, Siksha 'O' Anusandhan Deemed To Be University, Bhubaneswar-751030, Odisha, India

E-mail address: [2]alakanandatripathy@soa.ac.in

E-mail address: [3]sambit.swagatam22@outlook.com

E-mail address: [4]smitarath@soa.ac.in

E-mail address: [5]tripathyalok@gmail.com