Enhanced Cloud Storage Security Using ECC-AES A Hybrid Approach

Abhishek Kajal, Asst. Professor, CSE, Guru Jambheshwar University of Science &Technology, Hisar,India, abhishekkajal82@gmail.com

Gulshan, M.Tech Scholar, CSE, Guru Jambheshwar University of Science &Technology, Hisar, India, gulshanjat@gmail.com

Abstract: Data integrity in the storage model of cloud computing is a big security concern. This could be because of the Multiple locations where the data might be residing. After that privacy protection and security of this spread out data could be at any stake. The data at such multiple locations need to be secure in the cloud storage. What needs to be focused here is how a more secure model can be provided to the cloud architecture. Majorly, here a hybrid approach ECC-AES encryption algorithm is applied over the data. Based on this, further enhancement or improvement upon the data will be studied here.

Keywords: Cloud computing, Elliptic Curve Cryptography (ECC), AES algorithm, A hybrid approach ECC-AES, Cloud security, Cryptography.

I. INTRODUCTION

The cloud computing is an emerging field of computer science. It is pretty big and growing bigger every day. It is the process of remote servers on the internet to store, lookup and access all data instead of a nearest server or a PC. Here, servers need not be bought anymore. They can just be rented from the cloud provider for cost-effective services. Also, rented servers in the cloud don't need any monitoring or managing. This would now be the responsibility of Cloud Services Provider (CSP). When something is put away in the cloud, that implies it is put away on web servers, rather than on the nearby PC. It resembles having an additional hard drive [7].

One that, the client can get to anyplace and whenever associated with the web. Previously, the client had just a home PC and the product introduced on it. Presently the client can take documents anyplace, where he needs. All credits go to cloud-based applications called web applications, which run inside the internet browser. It is free and it doesn't require to install anything to use it and it allows to creates several different projects. This provides access to everything that is created in google docs from any computer or device with an internet connection. It only requires a connected device to access the cloud, the user can take that all multimedia files with him wherever the user goes. For example, if a user takes a photo on a mobile device and uploads it to a cloud-based photo storage services like mi cloud or Instagram, then it is accessible on any of the other devices like on a computer or even on TV. For example, a user can share his/her vacation photos with friends and family instantly. With the photos and audio-video data stored at the cloud, they don't need to worry about losing them to a computer malfunction [17] [22].

The commonly used cloud-based storage services like 'Microsoft' or 'google drive' take backup from your system If something wrong goes to the local computer then the data can be easily transferred from the storage services to another device. But here is another problem of data integrity. This could be because of the Multiple locations where the data might be residing. After that privacy protection and security of this spread out data could be at any stake. The data at such multiple locations need to be secure in the cloud storage. What needs to be focused here is how a more secure model can be provided to the cloud architecture. Many cloud storage models are presented to provide the more secure model. Most of them use an encryption algorithm. This encryption algorithm uses to encrypt the data on the user's computer and then that encrypted data is stored in the cloud. So that no one could breach the security in the middle of transmission. And also, the data will be secured at the cloud server also [18] [20].

II. EXISTING TECHNOLOGY

AES (Advanced Encryption Standard) is the replacement of the DES algorithm. The key size of DES was very small. And also, the algorithm itself was not very effective in both hardware point of view and software point of view. So, it was the time for NIST (National Institute of Standard and Technology) in which to announce a competition to replace this. And eventually, after a lot of

 DOI : 10.18231/2454-9150.2018.0593

filtering and debates, they have zero down on what is called Advanced Encryption Standard [16].

It is a block cipher, that means the string of the plain text needs to be chopped into blocks. The difference in RSA was that they were chopped into 64 bits pair block. And the AES is twice of this size i.e. 128 bits pair block. But the overall process is the same as AES which is a box that is fed with the first block with the key and a block of 128 bits of ciphertext is then achieved. In the end, a ciphertext remains which is as long as the plain text and every 128 bits have been encrypted with AES all using the same key [21].

Going a little deeper, it is found that this is the combination of their basic recognized primitives, substitution, transposition and bitwise operation. The minimum and the basic most used size of the key in AES is 128 bits [1].

AES consist of three types of keys:

a. 128 bits
b. 192 bits
c. 256 bits

To encrypt a message, the message needs to be supplied with a key, the AES encryption algorithm scrambles the message and outputs (hopefully) unrecognizable data [6].

To decrypt a message, scrambled data and the same key as before needs to be supplied. The AES decryption algorithm unscrambles the message and returns the original message [4].

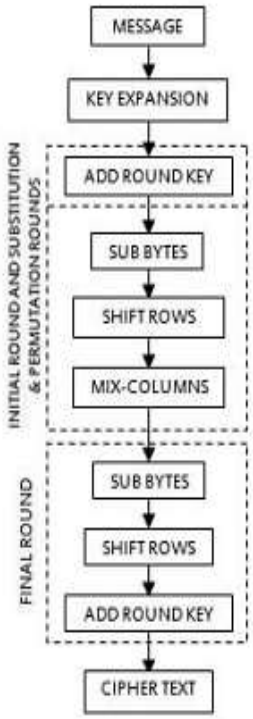

Fig.1. Workflow of AES algorithm.

III. LITERATURE SURVEY

As the use of cloud is increasing, the main topic of concern is the data security at the database server. Several types of research have been done and some are still ongoing on cloud data security. Here we talk about some major work in this field. K.Hajarathaiah and T.seshu [10] derive some solution to overcome the data loss accidents, that are generated at the transmission time. They used the TPA (third party auditor). Here they implement some dynamic operation like deletion, updating or append to recover the data and block the errors. Raman Kumar and Gurpreet Singh [9] developed a three-level secure design for stocking audio or video files which incorporate part-based authorized control, encoding, and sign confirmation. Subsequently, an improved secure powerful auditing method is derived, in which we can store information effectively at the cloud. Poonam and Deepali [3] proposed a scheme in which they use the Merkle Hash tree and AES algorithm to keep up the information trustworthiness at the distrustful servers. They had used a term TPA for the auditing and it works for the client for the integrity checking and also send the message back to the client. Khaba and M. Santhanalakshmi [8] implement a protocol that is used for data integrity checking. This data reading protocol can process a large batch file easily. They used the symmetric key encryption in the protocol. And also, the client can guarantee that every one of the information in the cloud must be in secured condition for its dependability. So here the size of data doesn't affect. Tao Jiang, Xiaofeng Chen, and Jianfeng Ma [11] presented a way to find out the collusion attack in the current plan. In addition to this, it gives a proficient public integrity method with secure gathering client renouncement which depends on vector responsibility and verifier-neighbourhood revocation group signature. It also supports people in general checking and proficient client revocation with properties, for example, confidently, effectiveness, accountable, and trackable of secure group user revocation. Babitha.M.P and K.R. Ramesh Babu [12] proposed a plan in which 128-bit Advanced Encryption Standard (AES) is utilized for expanded information security and classification. Information is encoded using AES and after that transferred on a cloud by means of this approach. Also, this scheme involves the use of Short Message Service (SMS) alert system to avoid unauthorized access to user data.

IV. PROPOSED SYSTEM A COMBINED APPROACH OF ECC-AES

Earlier when two users wanted to send a secret message then they would choose a scheme, for example, add one to each letter of the message. Then decrypting was as simple as subtracting that one off again. But if someone overhears them, then that whole system is ruined. The attempt to solve this problem have led us to create something called

 DOI : 10.18231/2454-9150.2018.0593

public key cryptography. So, in 1977, two separate sets of algorithms were introduced RSA and Diffie Hellman. These allowed us to have two different keys a public key and a private key [2].

And send the public key. Then the users need to take that public key combines it with the message to get an encrypted message. Then the user wants to send that message back to the bank. The user needs to use the private key to get back the original message. Now if there is an eavesdropper in the middle, they can see your public key and the encrypted message. But there is no way of figuring out or we can say, it is hard to figure out that 'what is the private key and what the message is?' [5].

So elliptic curve cryptography or ECC is a type of public key cryptography, which is presented in 1985. It is based on the somewhat esoteric topic of elliptic curve combined with some modular arithmetic. Some implementation uses the same principles as the earlier public key cryptosystem such as Diffie Hellman. But In the elliptical curve world, this creates a seemingly secure system [23].

In figure 2, they are symmetrical around the x-axis

The equation to generate these curves:

$\{(x, y) \in R2 \mid y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{\infty\}$

Some example of elliptic curves below:

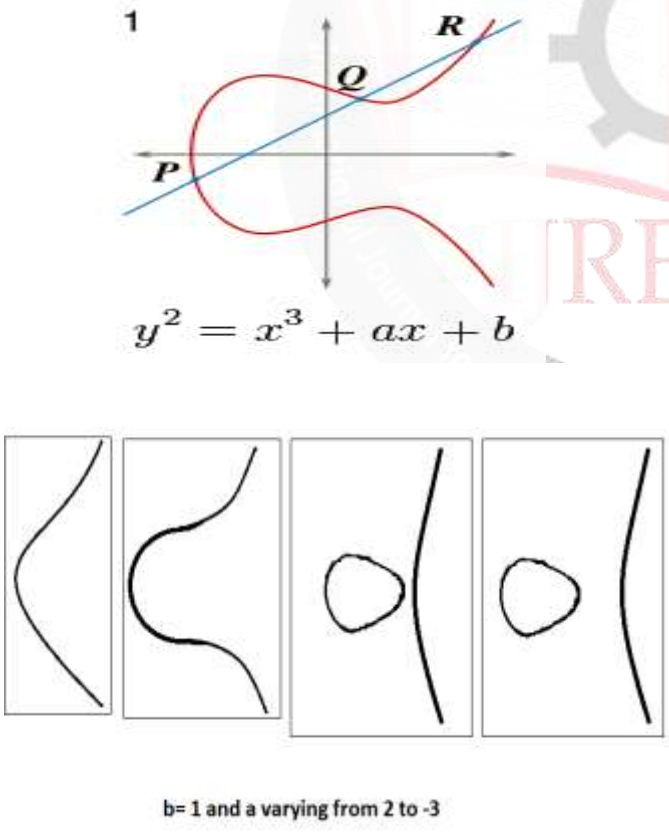

Fig.2. Some example of Elliptic curves.

Here a combined form of AES algorithm and Ecliptic curve cryptography is used to provide a better ciphertext in a more efficient time [25]. these two are different techniques and have different property. One is symmetric and the other is asymmetric. So here the public and private both keys are used. Firstly, both keys are used for encrypting the message. But here the AES is only applied for a single step i.e. converting the data to hexadecimal using the private key. And on the other hand, the ECC algorithm is applied to encrypt the same data. After that we combine the both encrypted forms. Now we get a final form of encryption. Similarly, for the decryption phase we apply the same method in reverse form. When the data is ready to upload firstly the data is encrypted using this combined form of ECC-AES and then uploaded [24].

V. TEST RESULTS

Now, a test was taken to compare these two algorithms i.e. the AES algorithm and a combined approach of ECC-AES. First of all, text data was taken and specify the key of size 128. Encryption on this text data was applied using the AES algorithm. The time taken for this encryption process was recorded. The original text data was converted into a ciphertext data after encryption. Next, the encrypted data (ciphertext) was decrypted to obtain the original text data. Time taken was again noted for this decryption process.

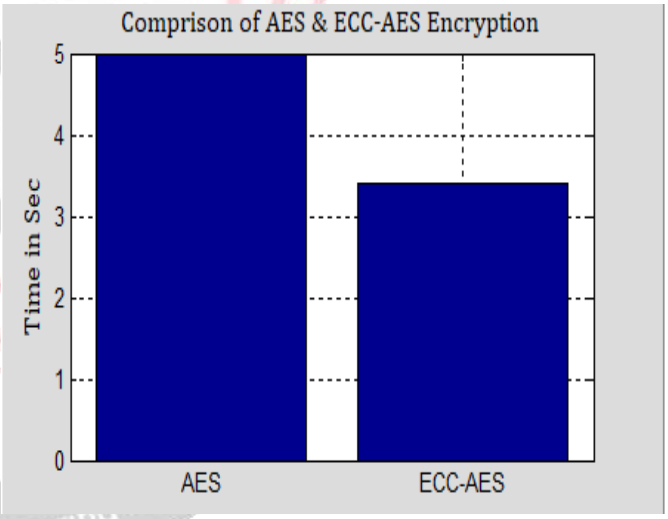

Fig.3 Comparison time for Encryption in AES and ECC-AES

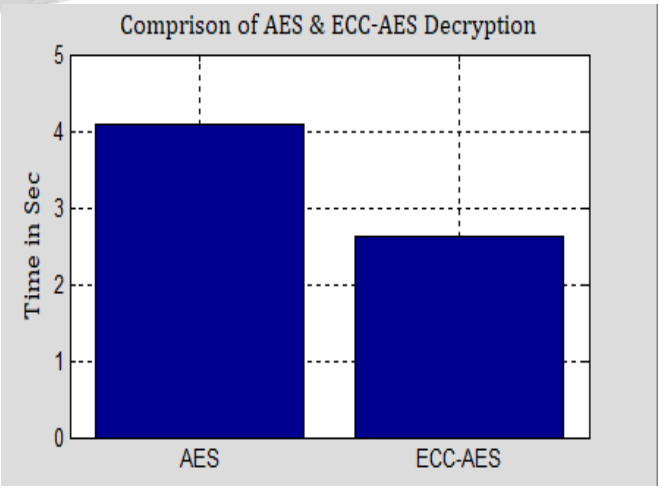

Fig.4 Comparison time for Decryption in AES and ECC-AES

 DOI : 10.18231/2454-9150.2018.0593

Similar tests were performed on another model that included the combination of the AES algorithm and ECC algorithm, termed as Hybrid ECC-AES Encryption and Decryption. The same text data was used to note the time taken for encryption and decryption processes.

A bar graph is shown in figure 3 here two bars are showing the encryption time taken by both the AES algorithm and ECC-AES algorithm. The time taken by ECC-AES is comparably low. And in figure 4 here two bars are showing the decryption time taken by both the AES algorithm and ECC-AES algorithm. Here also the time taken by ECC-AES is comparably low.

VI ANALYSIS OF TEST RESULT

For the final analysis of our test result, we compare the set of results of our hybrid scheme with the existing scheme (AES algorithm) for final confirmation, the tests were performed using different keys, namely, 64 bits, 128 bits, 192 bits and 256 bits. Both AES algorithm and Hybrid ECC-AES models were tested for a text data using these keys. At below the table shows all the values of time taken by both schemes. Also, here we can see the graph analysis of these values for better understanding.

Table 1. Encryption time in AES and ECC-AES

Key size (In bits)	AES encryption time (In sec)	ECC-AES encryption time (In sec)
64	-	2.43
128	3.73	2.46
192	3.67	2.47
256	3.75	2.51

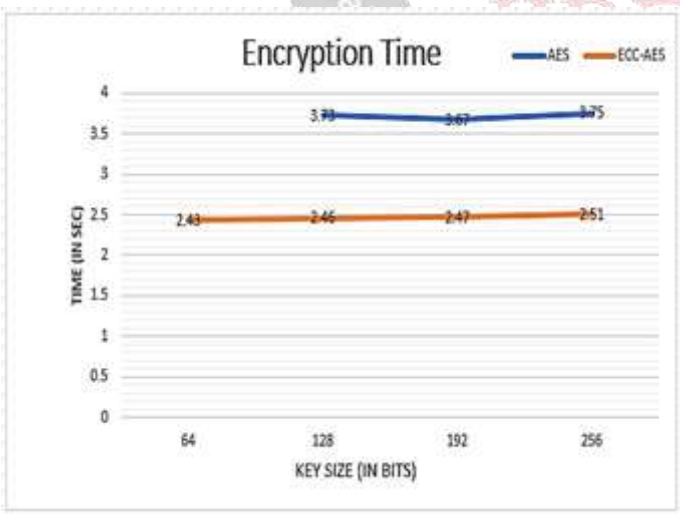

Fig.5 Comparison chart for encryption in AES and ECC-AES

Firstly, in encryption process using the 64-bit key, ECC-AES time was recorded as 2.43 seconds as shown in table 1. The 64-bit key doesn't work for the AES algorithm. For the 128-bit key, AES time was recorded as 3.73 and ECC-AES time was recorded as 2.46. For the 192-bit key, AES time was recorded as 3.67 and ECC-AES time was recorded as 2.47. for the 256-bit key, AES time was recorded as 3.75 and ECC-AES time was recorded as 2.51. The overall line chart depicts in figure 5 the time taken by AES and Hybrid ECC-AES models for the same text data for the encryption process. It was found that the Hybrid ECC-AES model took lesser time than the AES model.

Now for decryption process as shown in table 2 using the 64-bit key, ECC-AES time was recorded as 1.64 seconds. The 64-bit key again doesn't work for the AES algorithm. For the 128-bit key, AES time was recorded as 2.82 and ECC-AES time was recorded as 1.67. For the 192-bit key, AES time was recorded as 2.83 and ECC-AES time was recorded as 1.69. for the 256-bit key, AES time was recorded as 2.85 and ECC-AES time was recorded as 1.72.

Table 2. Decryption time in AES and ECC-AES

Key size (In bits)	AES decryption time (In sec)	ECC-AES decryption time (In sec)
64	-	1.64
128	2.82	1.67
192	2.83	1.69
256	2.85	1.72

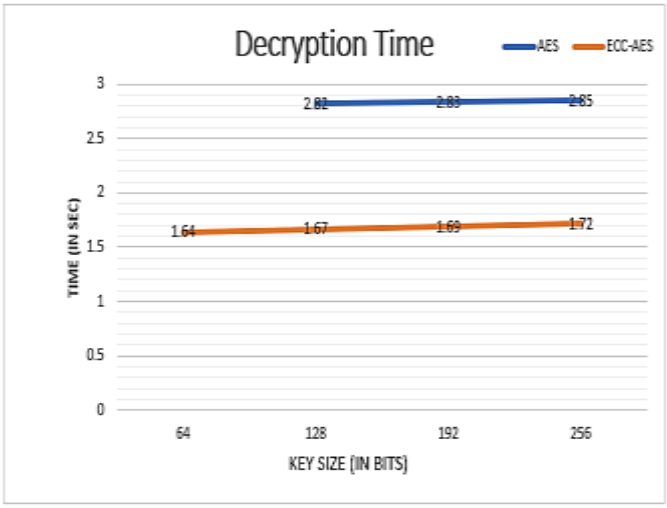

Fig.6 Comparison chart for Decryption in AES and ECC-AES

The overall line chart depicts in figure 6 the time taken by AES and Hybrid ECC-AES models for the same text data for the decryption process. It was found that the Hybrid ECC-AES model took lesser time than the AES model. Hence, the results were prominent in showing that the Hybrid ECC-AES approach takes lesser time in the process of encryption and decryption than the existing AES approach.

VII. CONCLUSION & FUTURE SCOPE

The ECC encryption scheme is very time efficient and require less computation and also less memory space. And on the other hand, AES provides a high security. So, this hybrid model gives a better security level by combining the features of both. The use of these two combined

 DOI : 10.18231/2454-9150.2018.0593

techniques makes the more complex system for an eavesdropper. This hybrid approach provides a faster process of both encrypting and decrypting a file than the standalone AES model. For future scope, the ECC encryption scheme can be combine with another similar encryption algorithm then the AES. Also, we can say that the 'ECC is the future of cryptography'. Its mathematical complexity and time efficiency give it a unique level.

REFERENCES

[1] V. R. Pancholi and B. P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," International Journal for Innovative Research in Science and Technology vol 2, Issue no.9, pp. 18-21, 2016.

[2] Ravi Gharshi and Suresha,"Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 7, July 2013.

[3] Poonam M. Pardeshi and Deepali R. Borade, "Improving Data Integrity for Data Storage Security in Cloud Computing", International Journal of Computer Science and Network Security (0975 – 8887), Volume 15 Issue No.7, pp. 61-67, July 2015.

[4] Gulshan And Abhishek Kajal, "A Review on Cloud Storage security", International journal of innovation in engineering research & management ISSN: 2348-4918, Volume: 05 Issue 02 Paper id-IJIERM-V- II-1130, April 2018.

[5] Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography.

[6] K Arul Jothy, K Sivakumar & Delsey M J, "Enhancing the security of the cloud computing with triple AES, PGP over SSL algorithms", International Journal of engineering sciences & research technology, February 2018.

[7] Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar "Efficient Cloud Computing with Secure Data Storage using AES" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015 ISSN (Online) 2278-1021

[8] Khaba M. V and M.Santhanalakshmi, " Remote Data Integrity Checking in Cloud Computing", International Journal on Recent and innovation trends in computing and communication, pg. 426-436, May 2017.

[9] Raman Kumar and Gurpreet Singh, "Analysis and Design of an Optimized Secure Auditing Protocol for storing data Dynamically in Cloud Computing", Materials Today: proceedings 5, pp. 1037-1047, 2016.

[10] K. Hajarathaiah, T. Seshu Chakravarthy, and G. Raphi, "Dynamic Operation Implementation in Storage of Cloud Computing", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3 Issue 3, pp. 463-469, March 2014.

[11] Tao Jiang, Xiaofeng Chen and Jianfeng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE transactions on computers, Volume: 65, Issue: 8, pp. 2363-2373, August 2016.

[12] Babitha.M.P and K.R. Ramesh Babu "Secure Cloud Storage Using AES Encryption", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (IIT), pp.859-864, June 2016.

[13] B. Nageswara Rao and B. Venkat Gopal, "Ensuring Distributed Accountability for Data Sharing in Cloud Using AES and SHA" International Journal of Innovative Research in Communication Engineering & Technology Volume no. 3, Issue no. 10, ISSN No.2655-4553, 2017.

[14] B. Priyadarshini and P. Parvathi, "Data Integrity in Cloud Storage", IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012), pp. 261-265, March 2012.

[15] T. Prasanthi, C. Balasubramanian, S. Kimsukha Selvi and K. Kala, "An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing", Proceedings of the World Congress on Engineering, 2014 Vol I, WCE 2014, London, U.K., ISSN: 2078-0966, pp. 678-688, July 2014.

[16] Prasanth SP and Gowtham B, "AES and DES Using Secure and Dynamic Data Storage in Cloud", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, pp. 401-407, January 2014.

[17] Ni Zhang, Di Liu and Yun-Yong Zhang, "A Research on Cloud Computing Security", IEEE International Conference on Information Technology and Application, pp. 370-373, 2013.

[18] Abdulaziz Alshammari, Sulaiman Alhaidari, Ali Alharbi and Mohamed Zohdy, "Security Threats and Challenges in Cloud Computing", IEEE 4th International Conference on Cyber Security and Cloud Computing, pp. 46-51, 2017.

[19] Wenjun Luo and Guojing Bai, "Ensuring the data integrity in cloud data storage", Proceedings of IEEE CCIS, pp. 240-243, 2011.

[20] Data integrity, https://en.wikipedia.org/wiki/Data_integrity.

[21] Advanced Encryption Standard, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[22] Cloud computing, http://en.wikipedia.org/wiki/Cloud_computing.

[23] The simple explanation for Elliptic Curve Cryptographic algorithm (ECC), https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/

[24] Samiksha Sharma and Vinay Chopra, "Analysis of AES encryption with ECC", Proceedings of International Interdisciplinary Conference On Engineering Science & Management, ISBN: 9788193137383, December 2016.

 DOI : 10.18231/2454-9150.2018.0593