PERFORMANCE OF EVALUATION FOR AES WITH ECC IN CLOUD ENVIRONMENT

D Bikshapathi, ABBA CHETHANA, EEDUNURI MURALIDHAR REDDY
4.KALYAN KUMAR, 5.M.CHITTI BABU
Assistant Professor, Department of Computer Engineering, Ellenki college of Engineering and Technonlogy, patelguda (vi), near BHEL ameenpur (m), Sangareddy Dist. Telangana 502319

.

ABSTRACT

During the day; Technology is Cloud, where people can share resources, services and information across the Internet. Due to information on the Internet, security is considered a major problem. The information should be protected by an unauthorized user and should be sent to a person with a private and confidential intent. On this proposed work, to provide a secure method, secure connection, authentication, confidentiality and third- party data protection in cloud computing. In the combination of the Advanced Encryption Standard (AES) and Cryptographic Curve Cryptography (ECC) analyzing of different parameters like storage, encryption time, decryption time and correlation. The results show that the impact of this integrated approach is more important than the other secure algorithms.

Keywords - Security, Advanced Encryption Standard, Elliptic Curve Cryptography, Cloud Computing, Cryptography Algorithms, Authentication, Privacy, Confidentially

I. INTRODUCTION

Cloud computing is becoming progressively fashionable in distributed computing environment. Cloud computing is the concept of using remote service through network using various resources. In cloud computing user can pay on the basis of resources usage as timely basis .In general term we can define it is a technology that provide hosting service over internet it is continuously developed and there are several major cloud providers such as Amazon, Google, Microsoft, Yahoo etc. Cloud computing is generally divided in to three segments are: “Application”, “Storage” and “connectivity” and each segment is used to service as a different service for a different purpose to use in different business.

The concept of cloud computing is linked closely with those of service model:

IaaS (Infrastructure as-a-services): It basically deals by providers to provide feature on demand utility.

PaaS (Platform as-a-services): It is used by developer for creating new application.

SaaS (software as-a service): It is provide application as a service on internet.

NaaS (Network as a Service): It provides directly to access to network infrastructure and securely.

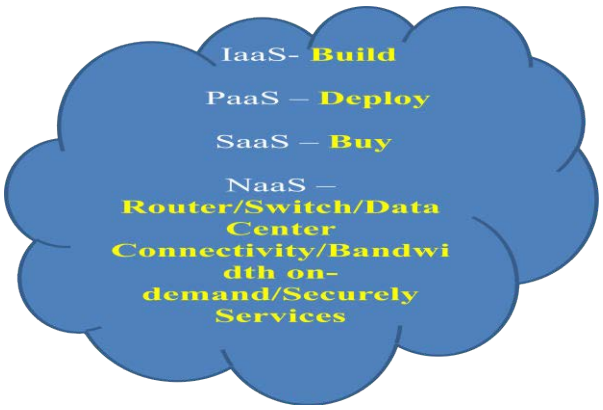


Fig: 1 Cloud Computing Services

1.1 Benefits of Cloud Computing:

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.11

☐ Cost Savings: Companies can reduce their spending and use their potential efficiently. This is the lowest car of the number of questions on the IT buildings to provide support.

☐ Scalability/Flexibility: Companies can start with a small start and produce more rapid shipping, and then return when needed. In addition, cloud computing allows companies to use more resources at high rates, to meet consumer demand.

☐ Reliability: Services that use multiple open websites may support business continuity and disaster recovery.

☐ Maintenance: Cloud service providers make system maintenance and access to the APIs that do not require installation on the PC, thereby reducing the need to reduce.

☐ Mobile Accessible: Mobile workers have increased productivity due to accessible infrastructure programs available.

1.2 CHALLENGES OF CLOUD COMPUTING Privacy of data: Data privacy is a basic problem of security in cloud computing. Most organizations feel very comfortable to put important data on their site with a space of space. Consumers are not aware of location data, data transfer, cloud functions, etc. Many organizations do not recognize the safety method provided by service providers.

Many questions are arising by consumers such as

☐ What are the organizations sharing services?

☐ How creation and back-up of files taking place.

☐ What happens to deleted files?

☐ What kind of customers can access data?

☐ Data location.

Confidentiality of data: Confidentiality relates to privacy information; Certificates that data is only visible to authorized users. It is very difficult because of the efficiency and many buildings to capture a number of users who share hardware, the software at the same time in the broadcast network. Confidentiality is the responsibility of the service provider. A common solution to encryption, there are a lot of confidential almasri and asymmetric available data, although encryption and crucifixion are a secret solution, there are many questions related to this

☐ Where is encryption and decryption enchanting place (client side or cloud side)

☐ How to analyze data in a written format.

☐ What threats when transferring customer data to the cloud?

☐ Any inappropriate data misuse by the service provider.

☐ Any unnecessary use of the key is the service provider.

Data Remanenece: Data should be removed from the cloud after the life cycle, or the memory must be changed or reused. Storage media storage does not remove previously written newspaper data, but can be accessed or restored later. There is no clear standard for renewal of last

media. Remanenece data makes holiday hardware services difficult. Most consumers are not known in the source and shared storage; as a result of this problem consumers are limited to one service provider. There are many techniques used to combat data. These methods are classified as cleaning, cleaning / disposal of blood or destruction. Clear paths include overwriting, cash sale, encryption, and media destruction.

Data integrity: The storage of information about losses or modifications by unauthorized users is called integrity data. Many organizations are involved in an app or platinum multi-tenancy, consumers who work on the same job can share information with any other unauthorized user sharing the application or platform in the cloud, which results in lawlessness. Since data is the basis for providing cloud computing services, such PaaS, SaaS, IaaS, DaaS and NaaS, keeping integrity of data is a fundamental foundation.

Transmission of data: Most data is converted between the buyer and the cloud. First the data was sent from the client website to the cloud, data is returned from the cloud to the client after the questions during the operation. Encryption is used to provide protection during data transfer. More time data is transferred without encryption because it takes a long time to encrypt and disable each operation and data. During the transfer the attacker can trace the connection, interrupt the data transfer, data losses, etc. The Homomorphic algorithm allows

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.11

you to operate data in a hidden way, although it may be possible to disrupt data transfer, data transfer, and other problems. Malicious Insiders: Malicious Insiders are authorized personnel, these users are selected to manage and maintain a cloud service provider. These users sometimes steal or cheat sensitive data from cloud organizations and transmit sensitive information to other organizations sharing the same cloud. These malicious traits can get paid for this cruel job. Sometimes a service provider cannot take action against employees.

1.3. SECURITY THREATS OF CLOUD COMPUTING

Cloud computing faces are the same time security threats currently available on existing computer platforms, networks, intranet, internets and companies. These threats, which are found at risk, come in many ways. The Cloud Security Alliance (Cloud Computing Alliance, 2010) performed a cloud-based investigation computing threats and found key threats:

- ☐ Attack on other clients
- ☐ Technological misuse
- ☐ Breakdown of something in Provider Security
- ☐ accessibility and trustworthiness Issues
- ☐ Integration of security systems and security customers
- ☐ Legal and regulatory problems
- ☐ Unprotected API
- ☐ The outside security system is broken
- ☐ Data Loss/Leakage
- ☐ Malicious(cruel) Insiders
- ☐ Unknown accident profile
- ☐ financial credit, Traffic Hijacking & Operation

II. LITERATURE SURVEY

P. Patil [3]. It presents a comparative analysis between the different measurement strategies and, in the end; it is perceived that AES requires a limit of the limit when compared to other measurement strategies and algorithms for safety security. P. Prajapati [4] compares between different encryption strategies such as AES, DES and RSA in the name of different mathematics as a requirement for memory and calculation time. AES requires less time to explore outside of RSA and DSA. P. Mahajan [5] used three DES strategies, AES and RSA cryptography strategies and compared their performance based on the measurement period. The separate digital results have shown that AES requires less time to encrypt and crucify. Dr. Smith Jones [3] proposes and uses a new way to repair the clouds through key-based cryptography, using the MD5 SHA-1 script to increase cloud security. B.Harikrishna [22] provides strongest authentication mechanism to a cloud client easily fit into any type of service in the cloud system.

R.Rivest, A.Shamir and L.Adleman [7] works with digital scanning and RSA cryptosystems. This research work was used for the digital signature of the RSA cryptographic system. It has also increased efficiency and security. Ravi shanka [8] increases the security of RSA cryptosystems depending on large quantities because it is difficult to break large amounts. The RSA algorithm provides security and performance. The collection function is always greater than the whole number. This paper is an RSA algorithm with powerful not in favor of brute force attack. B.Krishna shows how it allows it to provide authentication links to neighbors and speakers against the words and verification of the MD5 wishing process. Export passwords are expired; while [21] the MD5 support has been guaranteed to be able to maintain the online protocol of the web. B.Harikrishna [22] offers a straightforward way of signing the refreshing services that provide services throughout the any model.

III. PROPOSED WORK

For the proposed AES-192 and ECC, it is used to encrypt a file with a very strong lock. The input text file is converted to the AES algorithm, but the key used for the encryption process is generated by ECC and Diffie-Hellman to help unlock the ECC key encrypted and uploaded to the Cloud. After successful key agreement client would be able to decrypt the text message using that key to get the original text file. The main purpose of the proposed project is to secure the system so that only an authorized user can log on to the Cloud when an unauthorized user attempting to access our private Cloud can monitor and completely block the IP address and MAC of the device from which he is trying to access our private Cloud.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.11

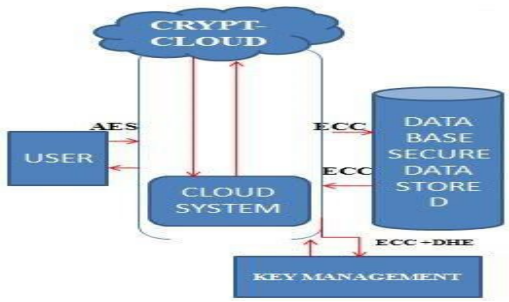


Fig 2: Proposed Model

Elliptic Curve Cryptography (ECC)

The ECC is called elliptic curve cryptography by Neil Koblitz and Vector Miller in 1985.The ECC provides better security for smaller sizes compared to other asymmetric algorithms. ECC 160-bit provides the same level of data security as RSA 1024-bit. High security levels can be found at an important size.

Measure the binary elliptic curve of the binary field written by-

$H^2 = N^3 + aN + b$

Key Generation: Primary invention is an essential part where it should create both a public key and a private key. The correspondent encrypts the message to the recipient's social circle and the recipient clicks the private key. Now we have to select a number within "m" width.

Use the following equity to generate a public key R = f * t

f = random number selected within width (1 to m).

't' is a point of curve.

'f' is the private key and 'R' is the public key.

Encryption

☐ Let 'l' be the message that, are sending, have to represent this message on the curve.

☐ Regard as 'l' have the point of "L" on the curve 'C'.

At random choose 'j' since [1 to (m-1)].

Two cipher texts determination be generated let it be

CP1 & CP2.

CP1 = F*T CP2 = L + F*R

CP1 and CP2 will be sending.

Decryption

To retrieve the message 'm' that was send to us,

L = CP2 – f * CP1

M is the original message that we have send.

Proof

How do to get back the message?

L = Cp2 – f * CP1

'L' can be represented as 'CP2 – f * CP1'

= CP2 – f * CP1 = (L + F* Q) – d * (f * t) (C2 = L + F * R and C1 = r* t)

= L + r * f * t – f * r *t (canceling out r* f * t)

= L (Original Message).

Advanced Encryption Standard (AES)

AES was announced in 2001 as the National Institute of Standards and Technology (NIST). AES should be used

for the encryption process for its security, efficiency and ease. AES is a symmetric encryption algorithm using the same key for both encryption and processing, known as symmetric block cipher. It uses three parts AES-128, AES-192 and AES-256 blocks. There are different processing cycles by block size such as 10 rounds, key lengths and block size of 4 128 bit keys, 12 round rounds by 6 key, and block 4 for 192 bit and 14 round keys, 8 words key and 4 block size for 256 bit key.

AES is announced as a federal information Processing standard by NIST (National Institutes of Standards and Technology) in 2001. AES is to be used encryption technique due to its high security, efficiency and simplicity. AES is Symmetric encryption algorithm which uses the same key for both encryption and decryption process and known as symmetric block cipher. It uses three block ciphers AES-128, AES-192 and AES-256. There are different rounds of processing according to the block size such as 10 rounds, key length and Block Size 4 words for 128- bit key, 12 rounds, key length 6 words and Block Size 4 for 192-bit key and 14 rounds, key length 8 words and Block Size 4 for 256-bit key.

Different steps for encrypting data with AES

- Round Key, Sub Bytes, Shift Rows and Mix Columns
- Initial Round

Add round key: Bitwise XOR technique is used to merge apiece byte of the position with the derived round key.

Different Rounds of Processing

1. Sub Bytes: Each byte has been replaced by the other access table.
2. Shift rows: This step is called the transposition step, where each row changes depending on the number of times you want.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.11

3. Mix columns: four Bytes of each column are combined in a state matrix

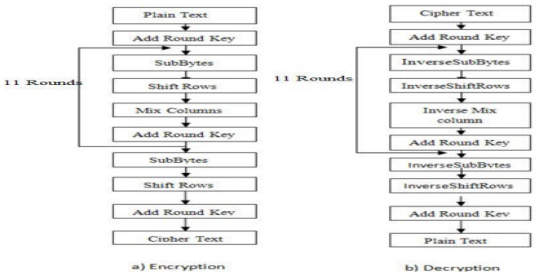


Fig 3: Encryption and Decryption in AES

Final Round: Sub Bytes, Shift Rows, Add Round Key and So, the final round will not have mixing of columns

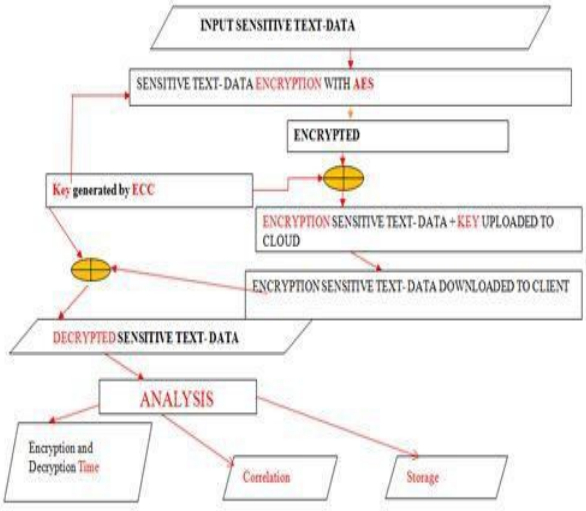


Fig: 4 flow chart for AES-ECC Encryption and Decryption.

IV. RESULTS AND ANALYSIS

Cryp-Cloud is a one of the Cloud platform, AES-ECC algorithm are implement to analyzing testing different file size, to obtained results of encryption storage, encryption and decryption time, and correlation.

Three metrics were taken to analyze the proposed methodology in Cryp-Cloud environment.

- ☐ Encryption Storage file
- ☐ Encryption time file
- ☐ Decryption time file

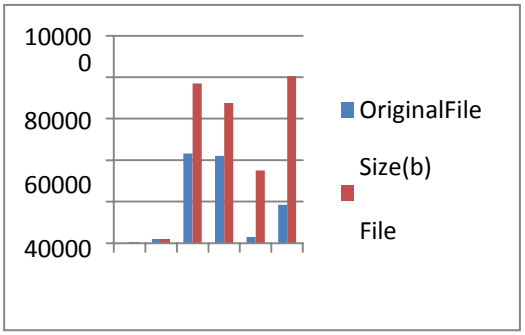
File Name	OriginalFileSize(b)	File Encrypted Size)(b)	EncryptionTime(ms)	DecryptionTime(ms)
1.Txt	17	359	0.062	0.062
b.Txt	1761	2068.48	0.125	0.047
2.Txt	43212	77004	0.063	0.047
a.txt	41984	67580	0.062	0.062
p.Txt	2959	35020	0.094	0.047
d.Txt	18432	80486	0.391	0.063

Table 1: Evaluation on the file storage, encrypted storage, encryption time and decryption times

4.1. Evaluating Encrypted File size of Different Files Below table 2, graph 1, shows original file size occupied less storage space and encrypted file size occupied large space. So, Storage is large than original file size for every set of input file. So any attackers does not hack the file.

FileName	Original File Size(b)	File Encrypted Size(b)
1.txt	17	359
b.txt	1761	2068.48
2.txt	43212	77004
a.txt	41984	67580
p.txt	2959	35020
d.txt	18432	80486

Table 2: File size original and encryption size



Graph 1: File size original and encryption size

4.2. Evaluating Encryption/Decryption Time of Different files

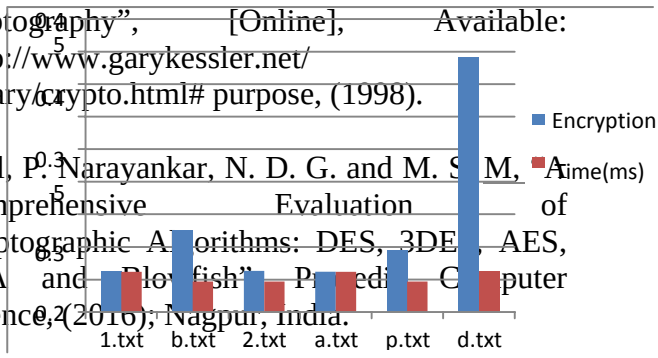
Below table 3, graph 2, shows the encryption and decryption time. Computation speed of algorithm is much high as it requires much less time for encryption and decryption

FileName	EncryptionTime(ms)	Decryption Time(ms)
1.txt	0.062	0.062
b.txt	0.125	0.047
2.txt	0.063	0.047

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.11

a.txt	0.062	0.062
p.txt	0.094	0.047
d.txt	0.391	0.063

Table3: encryption and decryption times



Graph 2: encryption and decryption times

V. CONCLUSION

Hybrid model combining of the AES and ECC algorithm, AES is a symmetric technique and ECC which is widely known as asymmetric technique to guard the communication from external risk. Various text file sizes are taken as input, the key is built using Elliptic Curve Cryptography (ECC), and encryption and encoding are performed using Advanced Encryption Standard (AES). AES and ECC reviews are based on different parameters such as file encryption size, encryption time, decryption time and correlation. The proposed hybrid algorithm process is very safe and integrated with AES-ECC provide much secure, break is difficult. The results show that the impact of this partnership is better than other algorithms.

VI. BIBLIOGRAPHY

[1] B. Hari Krishna, S. Kiran, G. Murali, R. Pradeep Kumar Reddy. "Security Issues in Service Model of Cloud Computing Environment", Procedia Computer Science, 2016.

[2] B. Harikrishna, S. Kiran, R. Pradeep kumar Reddy. "Protection on sensitive information in\ cloud — Cryptography algorithms", 2016 International Conference on Communication and Electronics Systems (ICCES), 2016.

[3] D. E. Denning, “Cryptography and Data Security”, Addison-Wesley Publishing Company, America, (1982).

[4] G. C. Kessler, “An overview of cryptography”, [Online], Available: ,http://www.garykessler.net/ library/crypto.html# purpose, (1998).

Patil, P. Narayankar, N. D. G. and M. S. M, A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish” Procedia Computer Science, (2016), Nagpur, India.

[6] P. Prajapati, N. Patel, R. Macwan, N. Kachhiya and P. Shah, “Comparative Analysis of DES, AES, RSA Encryption Algorithms”, International

[7] P. Mahajan and A. Sachdeva, “A study of Encryption algorithms AES, DES and RSA for security”, Global Journal of Computer Science and Technology, vol. 13, no. 15, (2013).

[8] Y. Wang and M. Hu, “Timing evaluation of the known cryptographic algorithms”, International Conference on Computational Intelligence and Security, (2009).

[9] 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, no. 09, (2016), pp. 18-21.

[10] P. Kumar and S. B. Rana, “Development of modified AES algorithm for data security”, Optik-International Journal for Light and Electron Optics, vol. 127, no. 04, (2016), pp. 2341-2345.

[11] A. K. Mandal, C. Parakash and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES”, Electrical, Electronics and Computer Science (SCEECS), (2012).

[12] A. A. Hasib and A. A. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography", Third International Conference on Convergence and Hybrid Information Technology, (2008).

[13] K. Rege, N. Goenka, P. Bhutada and S. Mane, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal of Computer Applications, vol. 71, no. 22, (2013).

[14] R. R. Ahirwal and M. Ahke, "Elliptic curve diffie- hellman key exchange algorithm for securing hypertext information on wide area network", International Journal of Computer Science and Information Technologies, vol. 4, no. 2, (2013), pp. 363-368.

[15] A. Pourali, M. V. Malakooti and M. H. Yektaie, "A Secure SMS Model in E-Commerce Payment using Combined AES and ECC Encryption Algorithms", The International Conference on Computing Technology and Information Management (ICCTIM), (2014).

[16] B. Ji, L. Wang and Q. Yang, "New Version of AES- ECC Encryption System Based on FPGA in WSNs", Journal of Software Engineering, vol. 9, no. 1, (2015), pp. 87-95.

[17] N. Jha and B. Patel, "Forward Secrecy For Google HTTPS using Elliptic Curve Diffie-Hellman Key", International Journal of Advanced Research in

Computer Engineering & Technology (IJARCET), vol. 1, no. 9, (2012).

[18] Dr.Smith Jones."AN EMPIRICAL CRYPTOGRAPHY ALGORITHM FOR CLOUD SECURITY BASED ON HASH ENCRYPTION", International Journal of Computing and Corporate Research ISSN (Online) : 2249-054X Volume 4 Issue
4 July 2014 International Manuscript ID : 2249054XV4I4072014-43.

[19] A method for obtaining digital signatures and public key cryptosystems, R.Rivest, A.Shamir and L.Adleman "communication of the association for computing machinery " 1978, pp 120-126.

[20] RSA algorithm using modified subset sum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011.

[21] Harikrishna, B. (2018). Network as a Service Model in Cloud Authentication by HMAC Algorithm.

[22] Harikrishna Bommala, S. Kiran (2018). Client Authentication as a Service in Microsoft Azure, vol 8, issues 2, IJEAT.