International Journal of Engineering &Technology, 7 (1.7) (2018) 84-86

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enforcing security in cloud environment using elliptic curve cryptography and third party auditing

Latha. K [1] *, Sheela. T [2]

[1] Research scholar, Faculty of computer science and engineering, Sathyabama University, Chennai-600119 Assistant Professor, Department of Computer Science and Engineering, Sri Sairam Engineering College, Ch – 44
[2] Professor & HOD, Dept of IT, Sri Sairam Engineering College, Chennai 600 044,Tamil Nadu, India
**Corresponding author E-mail: lathak.cse@sairam.edu.in*

Abstract

Cloud computing is the Internet-Based computing. In cloud computing, the resources will be shared, software and information will be provided to the computers and also other services on demand. The services are broadly classified in to three categories Infrastructure as a service (IAAS), Platform as a service (PAAS) and Software as a service (SAAS). Technical support of the cloud computing includes SOA and virtualization of hardware and software. Cloud service users need to be very curious in understanding the risk of data left in this new environment. Cryptographic algorithmic techniques are implemented to sign the data block before sending in to the cloud to empowering the security of the shared data within the cluster. This proposal supports the inclusion of new users to the cluster and an existing batch person can be discarded by sustaining the privacy including data backup and drop out based on the techniques called automatic key generation the revoked user will no longer have access to the data that he retained formerly. Hence dynamic data operations, public auditing, active group user nullification and data security can be achieved successfully. Thus, we are following the use of login with a secret key along with the security question for the user.

Keywords: *Data Left; Cryptographic Technique; Cloud Computing; Public Auditing; Dynamic Data.*

1. Introduction

Cloud Computing gets its name as an analogy for the internet. The internet is revealing in the network diagrams in the cloud computing, cloud icon is representing "All that other stuff" i.e. it makes the network work [1]. Protracted vision of the computing utility is called cloud computing, it enables the distribution of services over the internet [2]. Security is the major issue in Cloud Computing. Encrypted form of data will be stored in the cloud environment. Key factors for protecting data are Access Control, Data Auditing, Authentication, and Authorization [3]. At sometimes, the cloud service provider will be hiding the data corruption to maintain the repudiation. To avoiding this complication, we are introducing an effective TPA to auditing the user's outsourced data.

1.1. TPA- third party auditor

TPA is auditing efficiently in the cloud data storage [4]. It will not have any local copy of the data and it will not providing any additional on-line burden to cloud users.

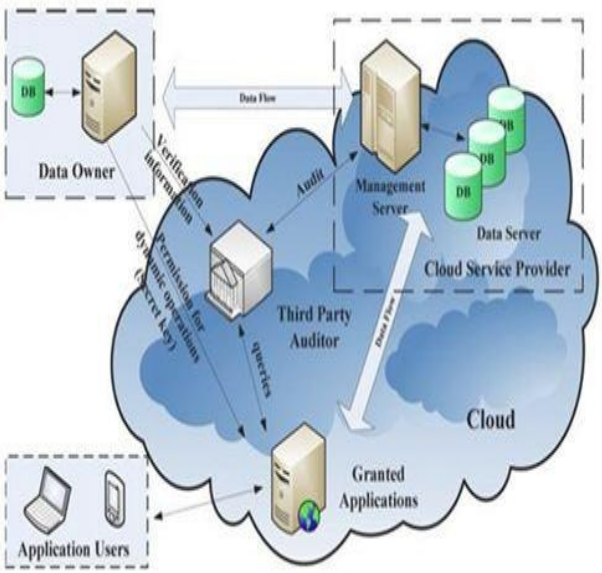


Fig. 1: Third-Party Auditor.

TPA will aid data holder to make sure that his data are safe in the cloud and management of data will be easy and less strain to the data owner [5]. Keys of ECC will be generating by using the properties of the ECC equation. It will not use any classical method of generation as the product of very large prime number. According to (Patel and Patel, 2012) std. TPA in the Cloud Environment should have following

Functionalities such as
i) No Data Leakage
ii) Integrity Verification
iii) High Performance
iv) Scalability

2. ECC algorithm (elliptic curve cryptography)

Equation of an elliptic curve is shown below, the terms which are used,
E -> Elliptic Curve
P -> Point on the curve
z -> limit which is maximum
(Must be a prime number)

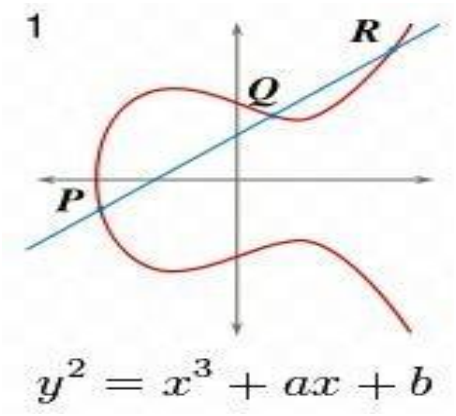


Fig. 2: Simple Elliptic Curve.

2.1. Key generation

Key generation is an essential part in which both public and private key are provoked. The sender wi encrypts the message with Public Key of receiver and the receiver decrypst its with Private Key.
Select a number 'S' within the range of 'z'.
Using the following equation and generating the public key.

Q = S * P

S = Selecting the random number from the range (1 - z-1). Consider P a point on the curve.
The public key and private key are 'Q' and 'S' respectively.

2.2. Encryption

Sending the message 'w'. Producing the message on the curve. Let us consider 'w' has the point 'W1' in the curve 'En'.
'k1' is selected randomly from the equation [1 – (z-1)].
Let us generating two different cipher texts C1 & C2.

C1 = k1 * P

C2 = W1 + k1 * Q

C1 and C2 will be communicated.

2.3. Decryption

Now we need to receive the message 'w' that was send,

W = C2 – S * C1

W is the original message which is sended before.
Proof:
Steps to go back the original message, W=C2-S*C1
'W' can be represented as 'C2 – S * C1'

C2 – S * C1 = (W1 + k1 * Q) – S * (k1 * P)

(C2 = W1 + k1 * Q and C1 = k1 * P)

= W1 + k1 * S * P – S * k 1*P (canceling out k1 * S * P)

= W1 (Original Message)

3. Implementation

3.1. User login

The set of action that will be executed by the user in the shared data within the cloud are as shown below in the following flowchart diagram.

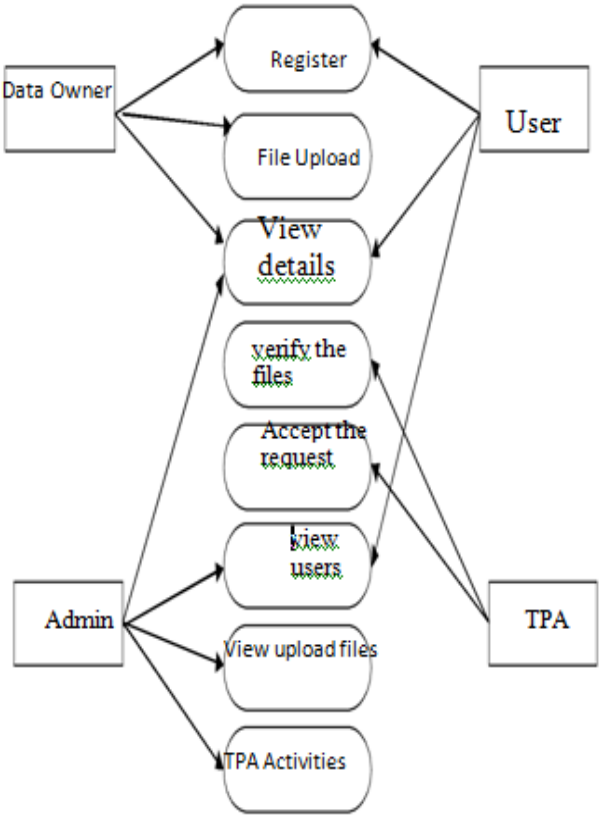


Fig. 3: Flowchart.

3.2. Registration

In registration, every user is required to be register into the cloud. As a result, these set of users will be permitted to login into the cloud server [6].

3.3. File upload

In this process, the user uploads a block of files into the cloud with encryption by using his or her private key. This excludes the illegal access of the cloud files.
This module allows the admin or the user to download the required file. The downloaded data needs to be decrypted using the private key of the owner of the corresponding file.

4. Comparison between the DES and ECC symmetric encryption techniques

Table 1: Comparison between the DES and ECC Symmetric Encryption Techniques

Parameter	ECC	DFS
Encryption method	Asymmetric	Symmetric
Key used	Public key and private key both are used encryption and decryption	Same key will be used for both encryption and decryption
Throughput	Higher	Lower
Security	very high	This is Proven inadequate
Power consumption	Low power consumption	Low power consumption
Key length	160,224,256,384,521	56
Security services provided	Confidentiality, Authentication Non-Repudiation	Confidentiality

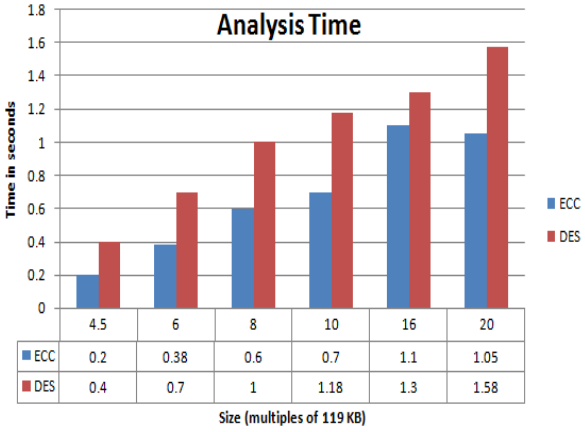
4.1. Encryption time based on entropy

Table 2: Encryption Time Based on Entropy

Size (multiples of 119 KB)	ECC (Time in secs)	DES (Time in secs)
4	0.20	0.40
6	0.38	0.70
8	0.60	1.00
1	0.70	1.18
1	1.10	1.30
2	1.05	1.58

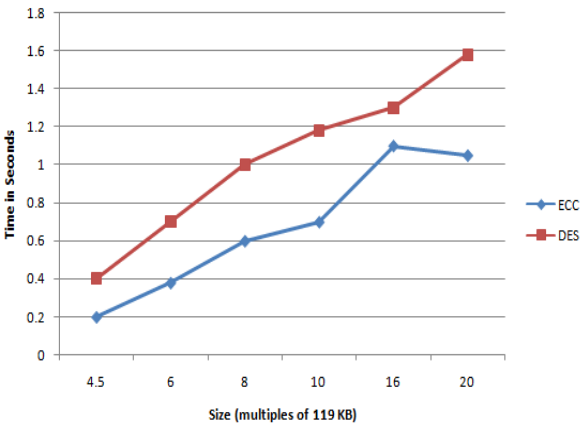
4.2. Chart: analysis of encryption time

Table 3: Encryption Time chart



4.3. Graph: analysis of encryption time

Table 4: Encryption Time chart



4.4. Disadvantages of existing system

The Actual system uses symmetric key algorithms such as AES and DES.AES and DES make use of a private key for cryptography. The bit size of the key in actual algorithms will be larger and takes more time for encryption and decryption. Hence this algorithm has less security.

4.5. Advantages of proposed system

ECC algorithm constructs faster, smaller and more efficient keys for Cryptography [6]. The level of security is large with 164-bit key whereas other algorithms use up to 1024-bit key. ECC perform with low computing power and consumes less battery resource [7].

5. Conclusion and future work

We established and delivered the output for Encryption time based on entropy, generating chart for analysis of Encryption time and graph for analysis of Encryption time. We compared the Encryption time between ECC and DES Algorithm. In future we plan to cover all the points in the Elliptic curve. Because due to time constraints we cannot cover all the points in the Elliptic curve. We also plan to improve the efficiency of the ECC Algorithm and also improve the speed of the algorithm.

References

[1] N. Shyamambika and N. Thillaiarasu., Attaining Integrity, Secured Data Sharing and Removal of Misbehaving Client in the Public Cloud using anExternal Agent and Secure Encryption Technique. Advances in Natural and Applied Sciences.

[2] Mell, P. and T. Grance, "Draft NIST working definition of cloud computing".

[3] Wang, C., Q. Wang, K. Ren and W. Lou, 2011. "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, 5(2): 220–232. https://doi.org/10.1109/TSC.2011.24.

[4] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[5] Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 https://doi.org/10.5121/ijnsa.2013.5502.

[6] Jachak, K.B., S.K. Korde, P.P. Ghorpade and G.J. Gagare, 2012. "Homomorphic Authentication with Random Masking Technique Ensuring Privacy &Security in Cloud Computing", BioinfoSecurity Informatics, 2-2: 49-52, ISSN. 2249-9423, 12.

[7] Yuan, J. and S. Yu, 2013. "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13. https://doi.org/10.1145/2484402.2484408.

[8] Boneh D., Di G., Ostrovsky R., Persiano G. (2004), "Public key encryption with keyword search", Advances in Cryptology-Eurocrypt, Springer, Berlin/Heidelberg, pp 506–522. https://doi.org/10.1007/978-3-540-24676-3_30.

[9] S. Subashini and V.Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, ,no.1, pp. 1 - 11, 2011. https://doi.org/10.1016/j.jnca.2010.07.006.

[10] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, Vol. 34, No. 1, 2011, pp. 1-11. https://doi.org/10.1016/j.jnca.2010.07.006.

[11] K. Periasamy and B. Latha, "The Enhancement Of Storage And Bandwidth Optimization Using DataDe-Duplication, in International Journal of Applied Engineering Research Volume 9, Number 20, 2014.