International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com
Reference ID: IJCS-234
Volume 5, Issue 1, No 16, 2017
ISSN: 2348-6600
PAGE NO: 1463-1467

Alagappa University, Karaikudi, India
15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr
ssicacr2017@gmail.com

Enhanced Security at Cloud Data with AES and ECC Cryptographic Algorithm

G.Shreedevi
Assistant Professor,
Dept. of Computer Science,
Vivekanandha Arts and Science College for Women,
Sankari, Salem Dt.

Abstract— Data privacy protection and data retrieval control are the challenging issues to be addressed in cloud computing. The paper presents away to provide the safety and security to the user's data, a Data security model that uses both AES and ECC Algorithm is proposed.By applying AES algorithm for digital signature on the message digestinstead of on the whole data to make the computations faster. Elliptic Curve Cryptography (ECC) was discovered as a mechanism for implementing public-key cryptography. In this work both digital signature scheme and public key cryptography are integrated to enhance the security level of Cloud.

Keywords: Data security, Hashing,AES algorithm, Digital Signature, ECC algorithm.

I. INTRODUCTION

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing [1] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of these benefits each and every organizations are moving their data to the cloud.So there is a need to protect that data against unauthorized access, modification or denial of services etc. Security goals of data include three points namely: Availability Confidentiality, and Integrity.Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3)Hashing. Integrity of data is ensured by hashing algorithms. In this paper the ECC algorithm and AES algorithm has been used to implement a data security model for cloud.

II. EXISTING ALGORITHMS FOR CLOUD SECURITY

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in this paper are;

1.AES algorithm

The AES encryption algorithm is a block cipher that uses an encryption key and several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AESencryption the block is 128 bits, or 16 bytes, in length. Theterm “rounds” refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key.AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. An encryption key is simply a binary string of data used in the encryption process.

A. *Characteristics of AES*

AES encryption algorithm is faster, more efficient and superior in terms of time consumption (encryption/decryption) and throughput under the scenario of data transfer.

TABLE I

Key Length	128,192 or 256
Block Size	128,192 or 256
Cipher Text	Symmetric Block Cipher
Security	Considered Secure
Speed	Very fast
Cryptanalysis resistance	VeryStrong against differential,truncated Differential, linear interpolation and square attack

2.Elliptic curve cryptosystem

Elliptic Curve Crypto system works on principles of elliptic curve. The equation of an elliptic curve over a field K considered in our work is given as,

$y^2 = x^3 + ax + b$ (1)

where, x, y = coordinates.a, b = elements of K. There are three steps in the process i.e., key generation, encryption and decryption.

A. *Encryption*

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. Consider ‘m’ as the point ‘M’ on the curve ‘E’. Randomly select ‘k’ from [1 - (n-1)].Cipher texts will be generated after encryption, let it be C1 and C2.

$C1 = k * p$ (3)

$C2 = M + k * Q$ (4)

B. Decryption

The message 'M' that was sent is written as following equation,

M = C2 - d * C1 (5)

C. Proof

The message 'M' can be obtained back using eq. (5)

C2 - d * c1 = (M + k * Q) - d * (k * p)

We have Q = d * p, by cancelling out k * d * p, we get M
(Original message).

ECC is better option when lot of users connects to cloud based services with small session time like cloud based storage. That's why ECC proposed as asymmetric encryption algorithm for cloud environment.

3. SHA-512

To achieve authentication and non-repudiation purpose within cloud computing environment digital signature has assumed great significance. There are various digital signature algorithms which involves the generation of message digest (hash).With respect to security concerns SHA-512 is more secure than MD5 and no claim of successful attacks with optimal time complexity on SHA-512 has been done so far.

III.LITERATURE SURVEY

The data security model using Two-Way handshake is a method which utilizes the homomorphic token with distributed verification of erasure-coded data and achieves the integration of storage correctness insurance and data error localization[2].
Sobol sequence method rely on erasure code for the availability, reliability of data and utilize token precomputation using Sobol Sequence to verify the integrity of erasure coded data rather than Pseudorandom Data in existing system, this scheme provides more security to user data stored in cloud computing[3].
In RSA cryptosystem Research Paper, they have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm in paper [4].
The semantic based access control model considers relationships among the entities in all domains of access control namely Subject (user), Object (Data/resource), Action (select, open, read, write) and so on, it is also shown how to reduce the semantic interrelationships into subsumption problem. This reduction facilitates the propagation of policies in these domains and also enhances time and space complexity of access control mechanisms [5].
Applying agent's method introduces agents to data security module in order to provide more reliable services [6]
A novel third party auditor scheme a third-party auditor which affords trustful authentication for user to operate their data security in cloud. The obvious advantage of this scheme is that the cloud

service provider can offer the functions which were provided by the traditional third party auditor and make it trustful. So it indeed reduces the constitution's complexity in Cloud Computing [7].

IV.PROPOSED MODEL AND PROPOSED SCHEME

A. *Proposed Model*

To provide the safety and security to the user's data, a Data security model that uses both AES and ECC Algorithm is proposed. AES for digital signature as shown in Fig.1.Elliptic Curve Cryptography (ECC) was discovered as a mechanism for implementing public-key cryptography. In this work both digital signature scheme and public key cryptography are integrated to enhance the security level of Cloud. The encryption of digital signature into cipher text is done as shown in Fig. 2

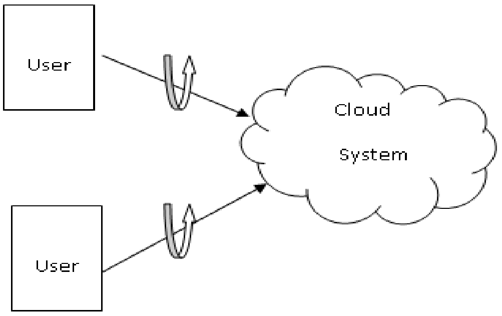

Fig.1. System Model

B. *Proposed Scheme*

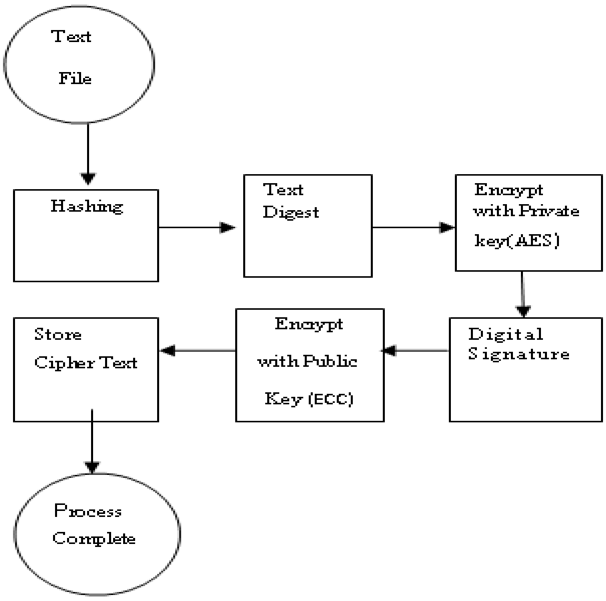

Fig. 2.Encryption of Digital signature into Cipher text

Step 1: In Digital Signature, the data/ document will be crunched down into few lines called as message digest by using hashing algorithm.
Step 2: The message digest is encrypted with private key implementing AES Algorithm to produce digital signature.
Step 3: Using Elliptic curve Algorithm, digitally signed signature is encrypted with public key.
Step 4: Receiverwill decrypt the digital signature into message digest using public key and the cipher text to plain text with his private key.

V.CONCLUSION

In this Paper, a more effective and flexible data security model is proposed to address the storage security issues associated with the data stored in Cloud. Also Integration of AES&Elliptic curve cryptosystems and digital signature will improve the security level provided to the user's data in the Cloud. ECC uses the smaller key sizes that involves less complexity but provides the same level of security as other public-key cryptosystems which uses larger key sizes involving greater complexity. TheAES algorithm is an excellent choice for encryption, since it is considered more secure. The clients can privately store data or share data with group users in a secure way. The cloud architecture proposed is going to be cost-effective forany organizations.

REFERENCES

[1] Yashpalsinh Jadeja, Kirit Modi," Cloud Computing - Concepts, Architecture and Challenges", 2012 International Conference on Computing, Electronics and Electrical Technologies, 978-1-4673-0210-4/12/.

[2] M.R Tribhuwan, V.A Buyar, Shabana pirzade,"Ensuring data security in Cloud Computing through Two-Way Handshake Based on token Management",2010 International Conference on Advances in Recent Technologies in Communication and Computing,978-0-7695-4201-0/10.

[3] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam," Ensuring Data Storage Security in Cloud Computing using Sobol Sequence",2010 1st International Conference on Parallel, Distributed and Grid Computing, 978-1-4244-7674-9/10.

[4] Uma Somani, Kanika Lakhani, Manish Mundra, " Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing",2010 1st International Conference on Parallel, Distributed and Grid Computing, 978-1-4244-7674-9/10.

[5] M. Auxilia, K. Raja,"A Semantic-Based Access Control for Ensuring Data Security in Cloud Computing", 2012 International Conference on Radar, Communication and Computing, 978-1-4673-2758-9/12.

[6] Feng-qing Zhang, Dian-Yuan Han, "Applying Agents to the Data Security in Cloud Computing", 2012 International Conference on ComputerScience and Information Processing,978-1-4673-1411-4/12.

[7] Shuai Han, Jianchuan Xing," Ensuring Data Storage Security througha Novel Third Party Auditor Scheme In Cloud Computing"Proceedingsof IEEE CCIS2011, 978-1-61284-204-2/11.