ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Data Security in Cloud Using Elliptic Curve Crytography

Puneetha C[1], Dr. M Dakshayini[2]

PG Student, Dept. of Information Science & Engineering, B.M.S.C.E, Karnataka, Bangalore,India[1]

Professor, Dept. of Information Science & Engineering, B.M.S.C.E, Karnataka, Bangalore,India[2]

ABSTRACT: Cloud Computing is a conceptual service based technology which is used by many organizations widely nowadays. As different types of normal data and also secret data are stored in the cloud, the client expects the cloud managing system to protect their data by providing security and maintaining secrecy. Data privacy protection and data retrieval control are the challenging issues to be addressed in cloud computing. Cloud system provides an innovative model for organizations to adopt IT services without upfront investment. Despite the gains achieved from cloud computing, the organizations hesitate in adopting Cloud due to security issues and challenges associated with it. Hence to address these issues, in this paper we propose a proficient data security model using ECC algorithm.

KEYWORDS: Data security, Hashing, Digital Signature, ECC algorithm.

I. INTRODUCTION

Cloud computing [1] is defined as a model for enabling, 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.Cloud computing interconnects the large-scale computing resources to integrate, and provide resources as a service to users(fig 1). Users are allowed on demand access to virtual computers, without the need to consider the complexities of the underlying hardware implementation and its management, greatly reducing the user's investment. The cloud computing applications and research continue to advance the development of cloud facing many critical issues, and bear the brunt of security issues and, the growing popularity of cloud computing but the security issues have restricted its importance in development.

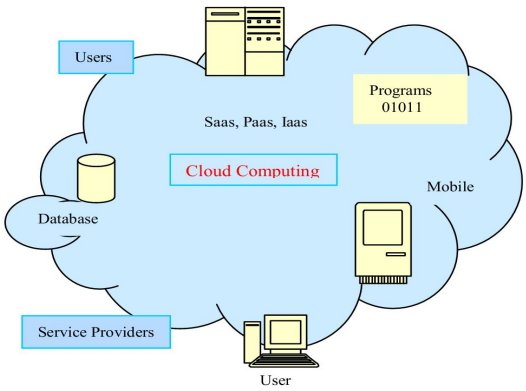

Fig. 1Cloud Computing

Recently, Amazon, Google and other cloud computing sponsors faced a variety of security incidents which contributed for people's fears. For example, in March 2009, Google place a large number of user files leak, in February 2009 and July, Amazon's "Simple Storage Service (simple storage service, called S3)" depends on two break lead to a single storage network Service's website was forced to a standstill, etc [2]. Thus, to make businesses and organizations

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

with huge application of cloud computing platform, to safely manage and deliver their data in the cloud, we must fully analyze and address the cloud computing security issues. In the present work the ECC algorithm has been used to implement a data security model for cloud.

The organization of the rest of the paper is as follows:Literature Survey of security issues is dealt in Section 2. Section 3 describes the Proposed Model. Section 4 focuses on internal working of model. Section 5 presents Conclusion and Future Work and Finally, the References.

II. LITERATURE SURVEY

Number of data security models have been developed to address the data security issues in cloud computing. 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, i.e., the identification of misbehaving server(s)[3]. 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. Theperformance analysis shows that scheme is more secure than existing system against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks [4]. In public auditing to support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient[5].In RSA cryptosystem Research Paper, they have tried to assess Cloud Storage Methodology andData Security in cloud by theImplementation of digital signature with RSA algorithm in paper [6]. Recently, the model which uses computational intelligence performance was proposed, computational intelligence (CI) is a mathematical modeling technique of cloud computing, which are vitally importance to simplifying the complex system and designing proactive and adaptive system in a dynamic and complex environment towards data security [7]. 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[8]. Applying agents method introduces agents to data security module in order to providemore reliable services[9]. A novel third party auditor scheme a thirdparty auditor which affords trustful authenticationfor 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 [10]. Ensuring data security is the common aim for all the above categories of security model.

III. PROPOSED MODEL AND ALGORITHM

A. Proposed Model

In order to provide the safety and security assurance to the users data, we propose a Data security model that uses Elliptic curve cryptosystem for digital signature as shown in Fig 2. Strength of the algorithm depends on the difficulty level of computing discrete logs in alarge prime modulus. A digital signature or digital signature scheme is a mathematicalscheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient a reason to believe that the message was created by a known sender, and that it was not altered in transit. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington)as an alternative 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. 3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

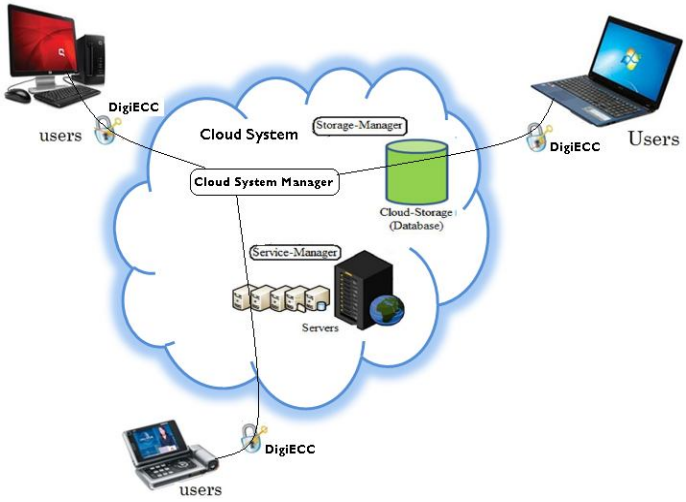

Fig. 2 Proposed Model

B. Proposed Algorithm

Step 1:In Digital Signature, the data/ document will be cruncheddown into few lines called as message digest by using hashing algorithm.

Step 2:The message digest is encrypted with private key to produce digital signature.

Step 3:Using Elliptic curve Algorithm,digitally signed signature is encrypted with receiver's public key.

Step 4:Receiver will decrypt the digital signature into message digest using sender's public key and the cipher text to plain text with his private key as shown in the fig 3.

Digital signatures are important to detect forgery and tampering

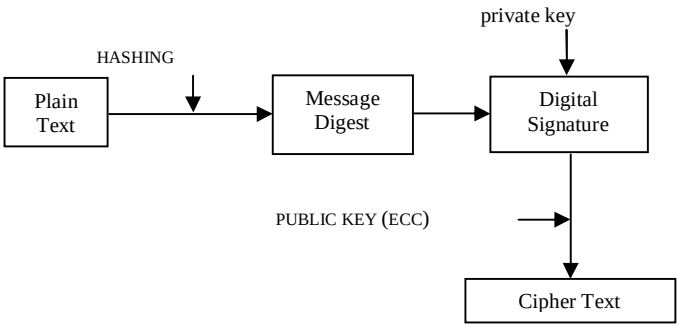

Fig. 3 Encryption of Digital Signature into Cipher text

IV. IMPLEMENTATION

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

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

where, x, y = co ordinates.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

a, b = elements of K.

There are three steps in the process i.e., key generation, encryption and decryption.

A. *Proposed Model*

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt using its private key. Now, we have to select a number **'d'** within the range of **'n'**.

we can generate the public key Using the following equation.

$$Q = d * p \quad (2)$$

where, d = The random number that we have selected within the range of (1 to n-1).
P= the point on the curve.
Q = the public key and 'd' is the private key.

B. *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 **C**1 and **C**2.

$$C1 = k * p \quad (3)$$

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

C. *Decryption*

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

$$M = C2 - d * C1 \quad (5)$$

D. *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).

V. SIMULATION AND RESULTS

The proposed security model is implemented using eclipse 3.7.2. Tomcat server is used to host the application, data is stored in cloud in encrypted format using elliptic curve cryptography during upload(Fig.4.1). The data downloaded(Fig.4.2) from cloud is verified using digital signature(Fig.4.3).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Fig.4.1 Data Encrypted and Stored in Cloud

Fig.4.2 Data Retrieved from Cloud

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

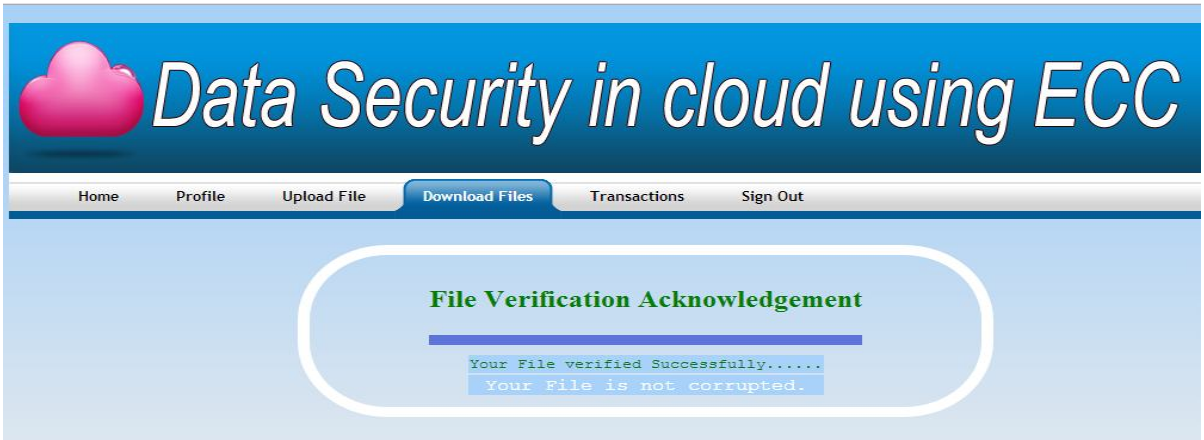

Fig.4.3 Verification Using Digital Signature

VI. CONCLUSION

In this work, A more effective and flexible data security model is proposed to address the storage security issues associated with the data stored in Cloud. The Strength of the algorithm due to the difficulty level used in computing discrete logs in a large prime modulus has increased the efficiency of the proposed model. Also Integration of Elliptic curve cryptosystems and digital signature has improved 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.

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. Yubo Tan , Xinlei Wang, " Research of Cloud Computing Data Security Technology",978-1-4577-1415-3/12,IEEE 2012.
3. 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.
4. 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.
5. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, " Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing",IEEE INFOCOM 2010 proceedings,978-1-4244-5837-0/10.
6. 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.
7. Chengliang Wang, Gebeyehu Belay Gebremeskal, "The Paradigm integration Of Computational intelligence Performance in cloud Computing Towards Data Security",2012 Fifth International Conference on Information and Computing Science,2160-7443/12.
8. 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.
9. Feng-qing Zhang, Dian-Yuan Han, "Applying Agents to the Data Security in Cloud Computing", 2012 International Conference on Computer Science and Information Processing,978-1-4673-1411-4/12.
10. Shuai Han, Jianchuan Xing," Ensuring Data Storage Security Through A Novel Third Party Auditor Scheme In Cloud Computing"Proceedings of IEEE CCIS2011, 978-1-61284-204-2/11.