ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (441-445), Month: April - June 2015, Available at: www.researchpublish.com

An Integrity Check For ECC-Based Data Storage in Cloud Computing Using SHA 512 Algorithm

[1]Sumith.K, [2]Gopal B

[1]Dept.Of CSE, Mangalore Institute of Technology and Engineering, Mangalore, India
[2]Assistant Professor, Dept. Of CSE, Mangalore Institute of Technology and Engineering, Mangalore, India

Abstract: **Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be main security threat. So, it is the responsibility of cloud service providers to ensure privacy and security of data on storage. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on cloud environment is maintained or not. Cloud computing is set of resources and services offered through the Internet. The rapid growth in field of cloud computing also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security, cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data and examining the utilization of cloud by the cloud computing vendors. This paper proposes a scheme to securely store and access of data via internet. We have used ECC based encryption scheme for storing the encrypted data in cloud because the use of ECC significantly reduces the computation cost, message size and transmission overhead over RSA based PKI as 160-bit key size in ECC provides comparable security with 1024-bit key in RSA. We have designed Secured Cloud Storage Framework (SCSF). This scheme can ensure the security and privacy of the data in the cloud architecture using various schemes. After storing the encrypted data in cloud, integrity of that is checked using SHA 512 algorithm. The integrity is checked by comparing the hash code which is generated before and after storing data in cloud.**

Keywords: **cloud storage, cloud computing, ECC, SHA 512, TPA**

I. INTRODUCTION

Cloud computing is a distributed computing style which offer integration of web services and data centers. There are several major cloud computing providers including Amazon, Google, Yahoo, Microsoft and others that are providing cloud computing services. Cloud computing is an emerging trend in the field of technology where resources, software and information is shared. Cloud computing provides a pay-per-use facility i.e. pay for only what the customer uses. This would reduce the customer's expenditure on hardware, software and other services [1]. Though there are various benefits of cloud computing like cost saving, scalability, reliability, maintenance still cloud computing has certain drawbacks like privacy, integrity, trust, DOS. As multiple users access information on cloud, the integrity and privacy of the information stored is at risk.. When data is sent by the user to be processed in the cloud; the control of the data is given to a remote party that may not address security concerns of the user. As a user has no physical access to the data, he is unaware about the location of his data and is not sure whether the integrity of his data is maintained or compromised in cloud. It is important to ensure that the information being processed on cloud is secure and no tampering of information is done when previously unknown parties may be present. A framework is proposed to provide data integrity using TPA to guarantee the various users that their data is unaltered. The main service offered by the cloud is nothing but storage facility [4].

Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. The biggest problem faced by cloud is security, because data is stored in third party known as servers. So there is a possibility of attack from the hacker. Cloud storage companies invest a lot of money in security measures. Since all the data are in plaintext form. A scheme is proposed to build a trusted cloud storage system, which allow the user to store and access their data securely. In this first the data is encrypted at the user side and store in cloud. If data is needed, then directly download the data and then decrypt. Since the private key is owned by the user of the data, no one can decrypt the data, even though hackers can get the data through some approaches. This scheme can make users assure about the security of data stored in the cloud. So finally for checking whether the data is altered or tampered, data integrity mechanism is used.

The rest of paper is classified as follows: Section 2 discusses the related work, Section 3 describes the proposed model to provide integrity of data, Section 4 describes the algorithm used and Section 5 presents the conclusion for the work done till now.

II. RELATED WORKS

Cloud computing is an emerging trend in the field of technology. There are various issues related to cloud computing, major ones being the security and integrity of data. Many frameworks have been designed and many algorithms have been proposed to resolve such issues.

Cheng Hongbing, et al. (2012) [2], introduced a secure data storage scheme based on identity-based encryption and biometric authentication for cloud computing. In that they focused on the security concern of cloud computing and then propose an integrated data storage scheme for cloud computing. Finally, they compared the proposed scheme with other schemes through comprehensive analysis and simulation. But still it is subjected to security problems.

P.Sumalatha, et al. (2013) [3], states that digital signature authentication is investigated and analyzed. Digital Signature authentication is a mechanism to transfer secret information over networks securely. Digital signature is an electronic signature used for authentication of identity of parties in applications like E-commerce which are frequently involved in monetary transactions. Identity based cryptography can secure digital signature authentication besides ensuring integrity, confidentiality and non-repudiation. In fact it is an emerging technique which works in tandem with public key cryptography. It is more useful when compared to classical public key infrastructure.

Muhammad Adeel Javaid, et al. (2014) [5], states that security and privacy challenges that are exacerbated by the unique aspects of clouds are presented and how they're related to various delivery and deployment models are shown. It also discusses various approaches to address these challenges, existing solutions, and work needed to provide a trustworthy cloud computing environment.

Amandeep, et al. (2014) [6], were using RSA algorithm for encryption and decryption of data to store in cloud. This algorithm is very efficient, it is also providing good security for the data from hackers, but the key size used in RSA algorithm is of 1024 bits. Because of this reason, I am using ECC algorithm which uses a key size of only 160 bits to provide the same level of security.

III. PROPOSED MODEL

This section defines the proposed framework to provide data integrity in cloud system. Proposed framework is shown in Figure 1 and has following three main roles:

- ***Users*** - who will upload the data in cloud by making use of ECC encryption and downloads the decrypted format.
- ***Admin*** - who will create the users and assigns the username and password for the users.
- ***Third party auditor (TPA)*** - verifies the cloud server and checks whether there is any manipulation of user data by the cloud server. It is done by comparing the hash code generated before and after storing in cloud.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (441-445), Month: April - June 2015, Available at: www.researchpublish.com

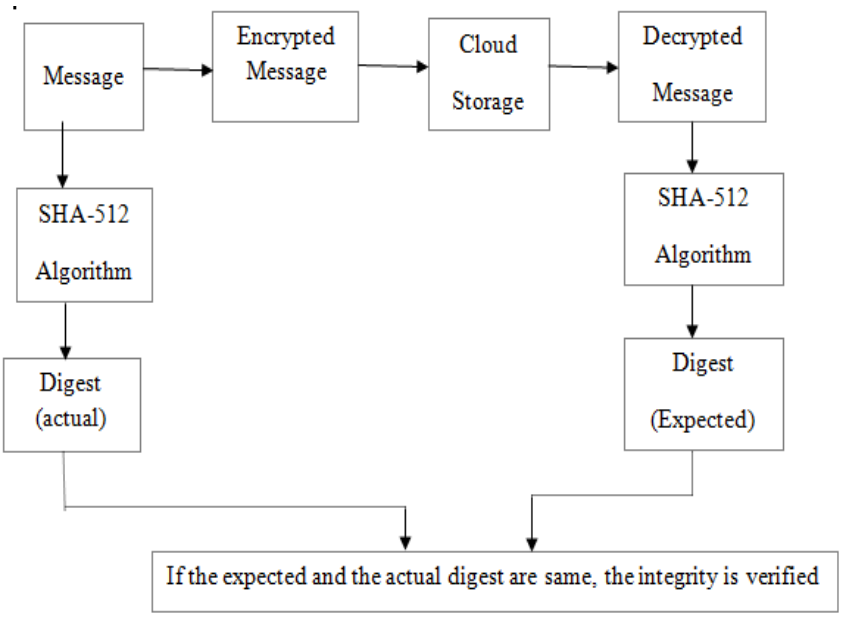

Fig 1: Proposed Framework

The application must request username and password for access. Only after authentication system will allow access. The system takes data, encrypt data, decrypt data and upload all these data into the cloud and it also create a hash value using SHA 512 for checking the integrity of the data. The data uploading will be encrypted using ECC algorithm. The following functions are mainly done by the system.

- **User registration**

The user should register with username and password. On the time of registration user need to give their personal information such as name, age, contact number, email id, username and password to login and upload the encrypted data.

- **Encryption and Decryption**

The system encrypts the data using with the public key in ECC encryption scheme. Then the data get stored in cloud. So while retrieving the data from cloud, it should be decrypted by making use of the private key.

- **Upload and Download**

The system uploads the file by making use of encryption scheme and downloads the file by making use of the decryption scheme.

- **Integrity checking**

After downloading the file, the TPA will be checking the integrity of the data by comparing the hash values obtained

IV. ALGORITHMS USED

A. Elliptic Curve Cryptosystem (ECC)

The elliptic curve cryptosystem was initially proposed by Koblitz and then Miller in 1985 to design public key cryptosystem and presently, it becomes an integral part of the modern cryptography. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography [7].

A brief introduction of ECC is given below:

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (441-445), Month: April - June 2015, Available at: www.researchpublish.com

Let E/F_p denotes an elliptic curve E over a prime finite field F_p, which can be defined by

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

where, $a, b \in F_p$ and the discriminate $D = 4a^3 + 27b^2 \neq 0$

The points on E/F_p together with an extra point O called the point at infinity used for additive identity form an additive group A as

$$A = \{(x, y) : x, y \in F_p, E(x, y) = 0\} \cup \{0\} \quad (2)$$

Let n, the order of A, is very large and it can be defined as $n \times G \bmod q = O$, where G is the generator of A. Also A be a cyclic additive group under the point addition "+" defined as $P + O = P$, where $P \in A$.

The scalar point multiplication over A can be defined as

$$tP = P + P + \cdots + P \text{ (t times)} \qquad (3)$$

If $P, Q \in A$, the addition $P + Q$ be a point $-R$ (whose inverse is R with only changing the sign of y coordinate value and lies on the curve) on the E/FP such that all the points P, Q and $-R$ lie on the straight line, i.e., the straight line cuts the curve at P, Q and $-R$ points. Note that if $P = Q$, it becomes a tangent at P or Q, which is assumed to intersect the curve at the point 0.

B. SHA 512(Secure Hash Algorithm)

SHA (Secure Hash Algorithm) refers to a family of NIST-approved cryptographic hash functions. The following table shows the various parameters of the different SHA hashing functions. The padded bits must be of size 1024 bits. Each 1024-bit message block is processed 80 rounds.

Table 1: SHA Parameters

Algorithm	*Message Size* (bits)	*Block Size* (bits)	*Word Size* (bits)	*Message Digest Size* (bits)	*Security* (bits)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

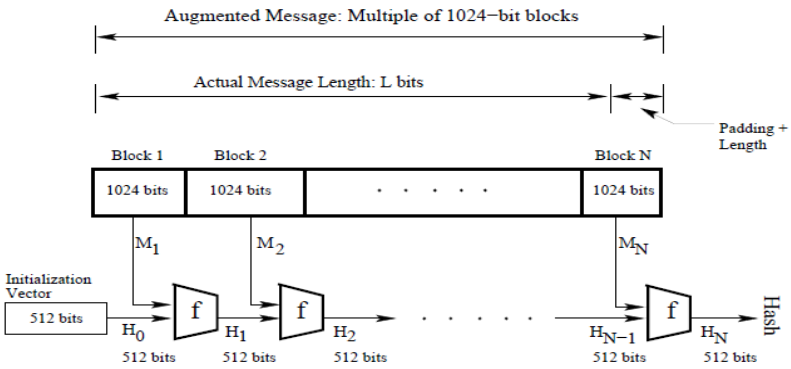

Fig 2: Overall Processing Steps of SHA 512

V. CONCLUSION

In this paper, we design a system showing cloud architecture, user and TPA that provide integrity proofs. Cloud Computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. As market grows the threat on data also grows. To protect the data from unauthorized access and to ensure that our data are intact we proposed a scheme, which solve the problem of integrity, unauthorized access, privacy and consistency. In this article we first present a network in which cloud architecture, users and TPA are shown after that we describe how file is retrieved. We then suggest a scheme for retrieval of file, encryption and decryption of file, how to check the integrity of our data from CSP and how to give control to TPA. Decrypted message is used to generate Hash value verified with stored value ensures data integrity. The clients can privately store data in a secure way. Later, we had defined the properties that will be given by our scheme. Further challenging issues for public auditing services that need to be focused on are discussed too. We believe that security in cloud computing is very much needed as data in the cloud storage are not secure and require lots of attention of user. The cloud architecture proposed is going to be cost-effective for institution lab setup and very small organizations.

REFERENCES

[1] XiaoChun YIN*, ZengGuang LIU**, Hoon Jae LEE "An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI", Feb 2014.

[2] CHENG Hongbing, RONG Chunming, TAN Zhenghua and ZENG Qingkai, "Identity Based Encryption and Biometric Authentication Scheme for Secure Data Access in Cloud Computing",Chinese Journal of Electronics Vol.21, No.2, Apr. 2012

[3] P.Sumalatha, Prof.B.Sathyanarayana, "A Review on Multi Level Identity Based Cryptography for Secure Digital Signature Authentication," International Journal of Computer Engineering and Applications, Volume V, Issue I, Jan.14

[4] Kun-Lin Tsai, Fang-YieLeu, Tien-Han Wu, Shin-shiuanChiou, Yu-Wei Liu, and Han-Yun Liu, "A Secure ECC-based Electronic Medical Record System", Journal of Internet Services and Information Security (JISIS), Volume 4, Isuue 1, 2014

[5] Muhammad AdeelJavaid, "Cloud Computing Security and Privacy",Horizon Research Publishing, 2014

[6] AmandeepKaur, SarpreetSingh"An Efficient data storage security algorithmusing RSA Algorithm"International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013

[7] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography .

Author's Profile:

Sumith K[1] completed the Bachelor's Degree in Information Science and Engineering from Visvesvaraya Technological University (VTU). Currently pursuing masters in Computer Network Engineering from MITE, Mangalore

Mr. Gopal B[2] received Master Degree in Computer Science and Engineering from NITK. He is currently working as Assistant Professor in the Department of Computer Science and Engineering, Mangalore Institute of Technology and Engineering.