Enhanced data security model for cloud using ECC algorithm and third party auditor

Niyati Jain[1], Priya Jain[2], Nikita Kapil[3]

[1, 2, 3] Department of Computer Science and Engineering
St. John College of Engineering and Technology
Palghar, Maharashtra, India

ABSTRACT-**With the invention of cloud, the days of keeping all the documents on the computer's hardware are gradually coming to an end. Today, people outsource their data at Cloud Service Provider (CSP)[1] who offers huge storage space at low cost. But as the data goes on cloud the user loses his control over the data and seeks for data security. Hence an efficient and effective method is needed to ensure integrity and confidentiality of outsourced data on un-trusted cloud servers. To address this issue the paper proposes Elliptic Curve Cryptography that owes a strong mathematical structure that raises the confidentiality level to an exceptionally high standard using minimum resources as compared to other existing algorithms like RSA, DES, AES etc., making it a first choice for devices with limited computing ability. Also paper proposes a method that allows Third Party Auditor to periodically verify the integrity of data stored at CSP without retrieving original data using md5 algorithm. The paper discusses key generation process, encryption and decryption of textual files using ECC algorithm along with a verification model which will address two crucial aspects of cloud security i.e. confidentiality and integrity.**

Keywords- Elliptic curve cryptography algorithm (*ECC*), Cloud Service Provider (CSP),Data confidentiality and integrity, RSA algorithm, MD5 Hashing algorithm, Third Party Auditor (TPA).

I. Introduction:

Cloud computing is a practice of using a network of remote servers hosted on the Internet to store, manage, and process data rather using a local server or a personal computer. There are several major cloud computing providers including Amazon, Google, Yahoo, Microsoft and others that are providing cloud computing services. Moving data into cloud offers great facilities to the users since they do not have to care about the maintenance cost and management cost of the hardware. But it has its drawbacks too. Once the data is uploaded on cloud a big question that troubles the client is how secure the data is on cloud? This question arises because the user loses his control over the data to CSP. Also the data now is on network platform which is prone to variety of attacks. Now it becomes prime essentiality to ensure confidentiality, integrity and availability of data on cloud .Confidentiality refers to keep data private. Measures undertaken to ensure confidentiality are designed to prevent private and confidential information from reaching the wrong people, while making sure that the right people can receive the data using encryption and access control techniques. Integrity is the assurance that information stored over the network can only be accessed, modified or fabricated by authorized users. Availability is performing necessary actions to ensure smooth functioning of operating system to make data available to the user whenever and wherever required. Thus, to satisfy the growing demand of cloud computing by corporate world it is essential to introduce a strong data security model to protect data against potential security threats. Also there is an exponential increase in thin clients trying to access cloud giving rise to new application domain. But due to limited computing resources and power constraints these devices need an algorithm that can work under limited computing resources. One stop solution to all the above mentioned issues is the use of ECC algorithm. Further involving third party auditor who periodically verifies the integrity of data on cloud by comparing the hash value using md5-hashing algorithm gives a cutting edge to proposed system over all other existing models.

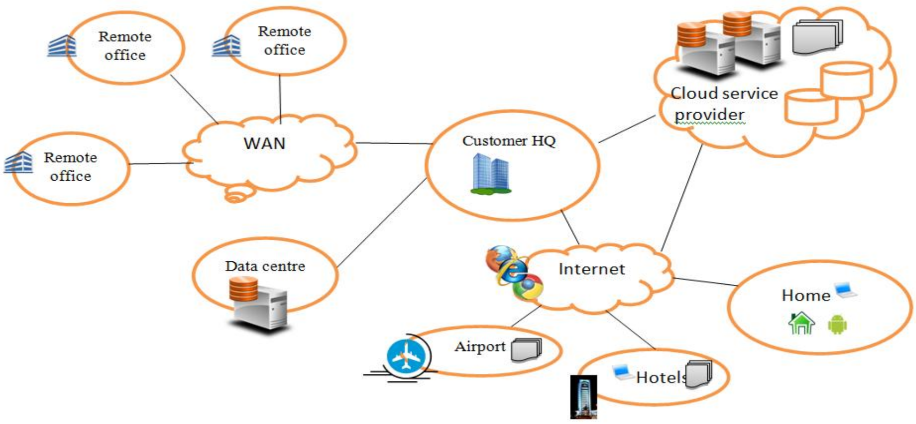

Fig 1: Cloud representation

Literature survey

Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties. Ravi Shankar Dhakar et al [5] talk about the "Modified RSA Encryption Algorithm (MREA)" where the talk about factorization in RSA cryptosystem, and their implementation compares the existing system and their system with key sizes up to 1024 bit. The authors claim their system to be better than existing system for the brute-force attack. Suli Wang et al [6] talk about the "File encryption and decryption system based on RSA algorithm" where they used RSA for encryption and decryption of files with smaller sizes. Maryam Savari et al [7] in "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application" compare the security of RSA 1024-bit key versus ECC 160- bit key sizes. P.R. Vijayalakshmi et al [8] in "Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol" compare ECC algorithm with 128 bits with that of RSA algorithm with 1024 bits key size. Kamlesh Gupta et al [9] in "ECC over RSA for Asymmetric Encryption: A Review" demonstrated the use ECC for portable devices and applications. Arjun Kumar et al [10] propose a method that allows user to store and access the data securely from the cloud storage in "Secure Storage and Access of Data in Cloud Computing". Xiao Zhang et al [11] talk about the physical security of data in data centers "Ensure Data Security in Cloud Storage". Somani, U et al [12] proposed implementation digital signature with RSA algorithm to enhance data security in cloud storage. Chakraborty, T.K et al [13] proposed a model for data security in cloud. Over last 10 years, a great deal of work has taken place to ensure that ECC meets these goals and is specified in an ever-increasing number of standards. Though there are several papers published on the comparison of ECC and RSA in terms of key sizes and security, this paper talks about the reduced key generation time, faster encryption and decryption time. In this work the used file are text files for the simulation i.e. encryption and decryption. This work compares the security of ECC in the key range of 160 - 512 bits and RSA key sizes ranging from 512 - 3072 bits. The simulation experiments compare the ECC and RSA at different levels of key sizes and block sizes.

Symmetric algorithm(bits)	RSA and DH (bit)	ECC (bit)
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table: Comparing key size of ECC with existing algorithms

II. Proposed Model

This section discusses briefly the use of Elliptic Curve Cryptography (ECC)-a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. ‘Domain parameters’ in ECC is an example of such constants.

The mathematical operations of ECC is defined over the elliptic curve

$$Y^2 = x^3 + ax + b, \text{ where } 4a^3 + 27b^2 \neq 0. \quad [21]$$

Each value of the ‘a’ and ‘b’ gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters ‘a’ and ‘b’, together with few more constants constitutes the domain parameter of ECC. The EC domain parameters are explained in section 9. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

Discrete Logarithm Problem

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

Pre-requisites to understand working of ECC:

Let P and Q be two points on the elliptic curve

- ADDING DISTINCT POINTS P AND Q
  P = (xP,yP) and Q = (xQ,yQ) are not negative of each other,
  P + Q = R where
  s = (yP - yQ) / (xP - xQ)
  xR = s2 - xP - xQ and yR = -yP + s(xP - xR)
  Note that s is the slope of the line through P and Q.

- DOUBLING THE POINT P
  When yP is not 0,
  2P = R where
  s = (3xP2 + a) / (2yP)
  xR = s2 - 2xP and yR = -yP + s(xP - xR)

ECC Domain Parameters

Elliptic curve parameters over the finite field Fp or F2m can be described by one set tuple:
T = (q, FR, a, b, G, n, h)

• q: the prime p or 2m that defines the field and at the same time decides the curve form;
• FR: the field representation, i.e., using which method to represent the elements in the field (polynomial basis or normal basis or subfield basis for F2m, Montgomery residue for Fp);
• a, b: the curve coefficient, depending on the security requirement;
• G: the base point also known as the generator point, G = (Gx, Gy),
• n: prime order of G ie. n is the smallest prime number such that nG=∞)
• h: cofactor ie. Number of points over the curve-it should be as small as possible.

A. Dealing with confidentiality aspect.

Key Generation

Key generation is an important part where we have to generate both public key and private key. The client will be encrypting the message with his public key and upload on cloud. When required client can download and decrypt the message using his private key.
1. Select a random integer d such that 1≤ d≤ n-1.
2. Compute Q = dG; d is the random private number, Q is the public key and G is the generator point on the curve.

Encryption

Let ‘m’ be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider ‘m’ has the point ‘M’ on the curve ‘E’. Randomly select ‘d’ from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$$C1 = d*P$$
$$C2 = M + d*Q$$

C1 and C2 will be send.

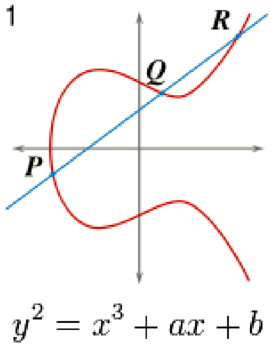

Fig 2: Standard ECC curve[14]

Decryption

We have to get back the message ‘m’ that was send to us,

$$M = C2 – d * C1$$

M is the original message that we have send.

B. Dealing with integrity aspect.

SHA-512

SHA-512 is a set of cryptographic hash functions. Cryptographic hash functions consists of mathematical operations that run on digital data by comparing the computed hash value generated by the algorithm to a known or expected hash value. With the help of this one can determine the data's integrity. In the proposed model, we are ensuring data integrity with the help of SHA-512 algorithm. This algorithm will be generating a hash value for the encrypted data which will be compared with the hash value of the corresponding data stored on cloud whenever the TPA wishes to perform data integrity check. If the generated hash value do not match with the data's hash value that means the data is been modified and the same will be notified to the user. If the hash value matches that means that the data is secured and integrity is maintained.

IV. System architecture

System Model

Cloud Data Storage Model The cloud storage model considering here is consists of three main components as illustrated in Fig.

1) **Cloud User**: The user, who can be an individual or an organization originally storing their data in cloud and accessing the data.

2**) Cloud Service Provider (CSP)**: The CSP, who manages cloud servers (CSs) and provides a paid storage space on its infrastructure to users as a service.

3) **Third Party Auditor (TPA) or Verifier**: the TPA or Verifier, who has expertise and capabilities that users may not have and verifies the integrity of outsourced data in cloud on behalf of users. Based on the audit result, the TPA could release an audit report to user.

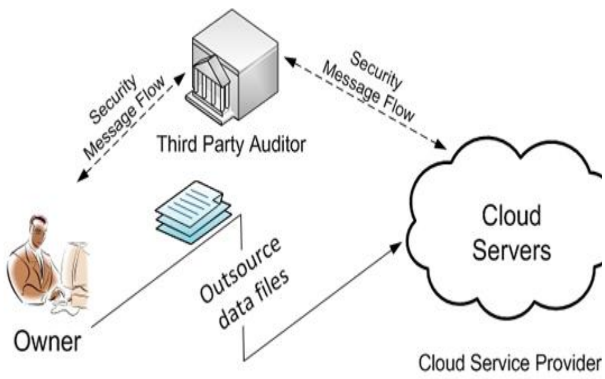

Fig 3: System architecture

Our system is designed to ensure security, confidentiality and integrity of data that is stored on cloud. First of all, the client who wants to store his data on cloud will register himself to the Cloud Service Provider (CSP) by providing all details. CSP will be then store all the details of the client like his id and password in the database of its own and auto-generate public and private key using ECC algorithm for each client which will be managed by an independent entity i.e. key repository. Generation of public key and private key is a backhand process Client will then login at cloud using his id and password after which initiation of file upload process will take place. Encryption of file chosen by client at the time of upload takes place using client's public key. This encrypted file will be stored on the cloud in the form of blocks. Whenever the user wishes to download the file, he will inform the CSP after which the file gets decrypted with the help of private key stored at key repository and the client gets back his original file. Another important component of the proposed system is Third Party Auditor(TPA). TPA stores the metadata of the file in its database which is obtained by applying MD5 hashing algorithm on encrypted blocks of file. TPA performs integrity check on the data periodically by comparing the checksum value of the blocks of data stored at cloud with metadata at TPA's database. If the value matches that means the data is secured and integrity of the data is maintained. However the TPA notifies the client each time irrespective of positive or negative result.

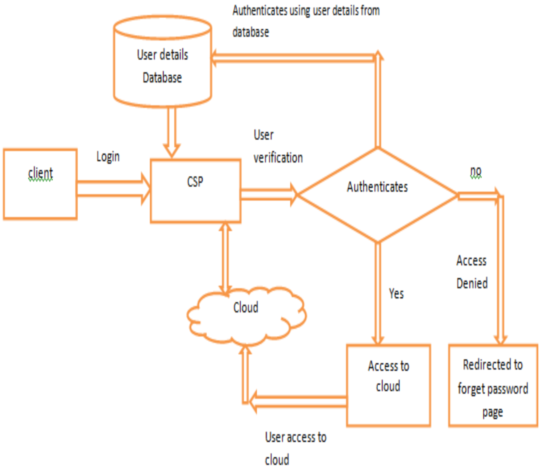

Fig 4: Schematic diagram showing login process

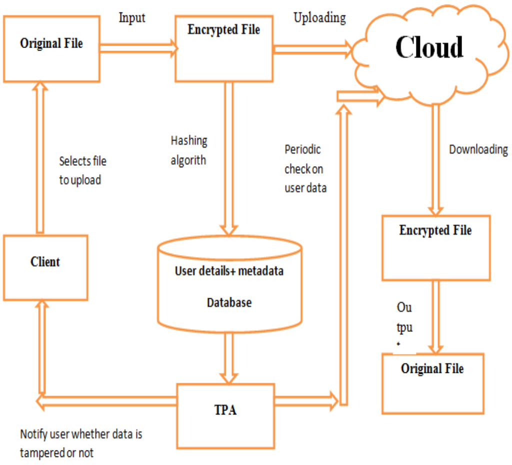

Fig 5: Schematic diagram showing upload and download process

V. Analysis

- Short key size: ECC employs a relatively short encryption key, a value that must be fed into the encryption algorithm to decode an encrypted message. This short key is faster and requires less computing power than other algorithms. For example, a 160-bit ECC encryption key provides the same security as a 1024-bit RSA encryption key and can be up to 15 times faster, depending on the platform on which it is implemented.

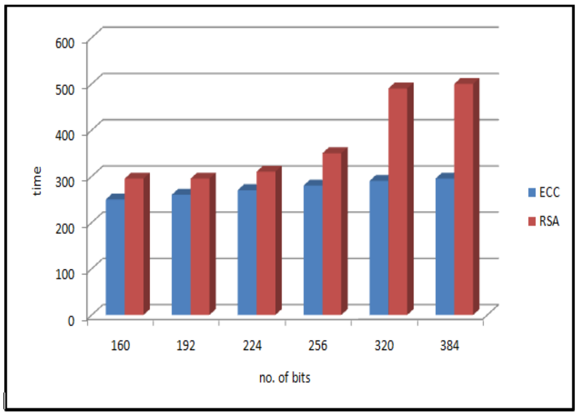

Fig 6: Comparison of key generation time(ms)

- More Complex: In spite of multiplication or exponentiation in finite field, ECC uses scalar multiplication. Solving Q= dP (utilized by ECC) is more difficult than solving factorization (used by RSA) and discrete logarithm (used by Diffie-Hellman (DH), EIGamal, Digital Signature Algorithm (DSA)).
- Power Consumption: ECC requires less power for its functioning so it is more suitable for low power applications such as handheld and mobile devices.
- Computational Efficiency: Implementing scalar multiplication in software and hardware is much more feasible than performing multiplications or exponentiations in them. As ECC makes use of scalar multiplications so it is much more computationally efficient than RSA and Diffie-Hellman (DH) public schemes. So we can say without any doubt that ECC is the stronger and the faster (efficient) amongst the present techniques.

VI. Conclusion

The cloud architecture proposed in this paper brings suitable way to store and access files provided with confidentiality, integrity and authentication properties. Data is encrypted before uploading to server storage, so confidentiality is preserved. On the receiver side the user can download and decrypt the files using the key stored in mail server at the time of encryption providing authenticity. Further the third party auditor reliefs user from the overhead of ensuring integrity of data by periodically verifying it. The proposed model proves that it is secure in terms of integrity and confidentiality through security analysis. Through, performance analysis and results proved that proposed scheme is efficient. Compared with previously proposed protocols, we have also proved that proposed scheme is more secure and efficient.

References:

[1]Ravi Gharshi ,Suresha “Enhancing Security in Cloud Storage using ECC Algorithm” International Journal of Science and Research (IJSR), India.

[2] PuneethaC1 ,Dr. M Dakshayini2 “Data Security in Cloud Using Elliptic Curve Cryptography” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, May 2014.

[3] Dr.Chander Kant, Yogesh Sharma “Enhanced Security Architecture for Cloud Data Security” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[4] Confidentiality, integrity, and availability (CIA triad): http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[5] Ravi Shankar Dhakar, Amit Kumar Gupta, "Modified RSA Encryption Algorithm (MREA)". Advanced Computing & Communication Technologies (ACCT), Second International Conference, 2012.

[6] Suli Wang, Ganlai Liu, "File encryption and decryption system based on RSA algorithm". Computational and Information Sciences (ICCIS), International Conference, 2011.

[7] Maryam Savari, Mohammad Montazerolzohour and Yeoh Eng Thiam,

"Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application". Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference, 2012.

[8] P.R. Vijayalakshmi, K. Bommanna Raja, "Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol". Computing, Communication and Applications (ICCCA), International Conference, 2012.

[9] Kamlesh Gupta, Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[10] Arjun Kumar, Byung Gook Lee, HoonJae Lee "Secure Storage and Access of Data in Cloud Computing". ICT Convergence (ICTC), International Conference, 2012

[11] Xiao Zhang, Hong-tao Du, Jian-quan Chen, Yi Lin, Leijie Zeng, "Ensure Data Security in Cloud Storage". Network Computing and Information Security (NCIS), International Conference, 2011.

[12] Somani, U, Lakhani, K, Mundra, M, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing". Parallel Distributed and Grid Computing (PDGC), 1st International Conference, 2010.

[13] Chakraborty, T.K.; Dhami, A.; Bansal, P.; Singh, T. "Enhanced public auditability & secure data storage in cloud computing". 3rd IEEE International Advance Computing Conference (IACC), 2013.

[14]A tutorial on Elliptic Curve Cryptography http://vanilla47.com/PDFs/Cryptography/Miscellenea/Eliptic%20Curve%20Cryptography/A_tutorial_of_elliptic_curve_cryptography.pdf

[15] RSA algorithm: http://searchsecurity.techtarget.com/definition/RSA

[16] Advantages and disadvantages of ECC: http://www.emc.com/emcplus/rsalabs/standardsinitiatives/advantages-and-disadvantages.html

[17]Diffie Hellman Key exchange Algorithm: http://searchsecurity.techtarget.com/definition/DiffieHellman-key-exchange

[18] Ravi Gharshi1 , Suresha2, “Enhancing Security in Cloud Storage using ECC Algorithm”. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 7, July 2013.

[19] Elliptic curve cryptography: https://www.youtube.com/watch?v=yDXiDOJgxmg

[20]Simple Tutorial on Elliptic Curve Cryptography:http://www.eis.mdx.ac.uk/staffpages/m_cheng/link/ecc_simple.pdf

[21] ECC tutorial: https://www.certicom.com/ecc

[22] Simple explanation for elliptic curve cryptography:https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/

[23] Advantages of ECC: http://arxiv.org/ftp/arxiv/papers/1109/1109.1877.pdf