International Journal of Engineering &Technology, 7 (1.7) (2018) 128-131

International Journal of Engineering & Technology

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

Research paper

Secured cryptographic data model for cloud

Antony Kumar K[1], Neeba E A[2] , Durai S[3], Ravikumar [3]

[1,3] AssistantProfessor, Department of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,Avadi,Chennai-600062
[1]Assistant Professor, Department of information Technology, Rajagiri School of Engineering & technology Rajagiri Valley P O, Kochi-682039, Kerala,India
**Corresponding author E-mail: antonykmr32@gmail.com*

Abstract

Cloud computing turns into the cutting edge engineering of IT Enterprise. Cloud essential key thought is to move the whole information models into the server farms where the portability and administration of information isn't completely reliable. The principle challenge in the cloud is the client information and framework application information is gotten to from the cloud supplier's premises; even security arrangements sent in the premises don't take care of the demand of the clients where the need differs. The on-request security arrangement is alluring, yet now days all the cloud suppliers are utilizing encryption systems to exchange the information and information ask for and reaction. Consequently in this proposition, another security show is proposed for the cloud model to give security highlights. The new thought is to apply elliptic curve cryptography to give the security highlights to on request information handling. This proposition explores the essential issue of cloud computing information security. At last the security demonstrate is conveyed in the cloud OS "open stack" and "cloud stack".

Keywords: *Elliptic Curve, Cloud stack*

1. Introduction

Cloud computing gives another method for administrations by sorting out different assets and giving them to clients in view of their requests. It likewise assumes a significant part in the cutting edge portable systems and administrations (5G) and Cyber-Physical and Social Computing (CPSC). Cloud computing and limit courses of action give customers and endeavors distinctive characteristics to store and process their data in outsider server farms that may be masterminded far from the client running in expel from over a city to over the world. Cloud computing relies on sharing of assets to accomplish continuance and economy of scale, like an utility (like the power framework) over a power organize. Putting away information in the cloud enormously diminishes capacity heap of clients and brings them get to comfort, in this manner it has turned out to be a standout amongst the most imperative cloud administrations. Potential outcomes ensure that, Cloud computing empowers associations to avoid direct foundation costs (e.g. acquiring servers). In like manner, it draws in relationship to center around their center organizations as opposed to contributing vitality and backings on PC foundation. Cloud computing empowers endeavors to get their applications up and running speedier, with upgraded sensibility and less support. Nevertheless, concerns are beginning to make about how safe Cloud is? as more information on individuals and associations are being placed in the cloud. Neglects to all the buildup encompassing the cloud, undertaking clients are as yet unwilling to put their business in the cloud. One of the genuine concerns which reduces the improvement of Cloud figuring is security and hindrance with information security and data assurance continue contaminating the market. Cloud data stockpiling expands the peril of information spillage and nonsensical get to. The design of cloud represents certain threats to the security of the current advancements when sent in a cloud situation. Cloud benefit clients should be caution in translating the dangers of information interruption in this new environment.[1] The security worries as for Cloud computing are end-client information security, arrange activity, document frameworks and host machine security which can be tended to with the assistance of cryptography to an extensive level.

What is cryptography?

Cryptography or cryptology is the training and investigation of methods for safe correspondence inside seeing untouchables called enemies.[2] More by and large, cryptography is taut in with emerging and separating traditions that counteract outcasts or individuals all in all from examining secretive communications;[3] dissimilar viewpoints in information security, for example, data secrecy, data uprightness, verification, and non-refutation[4] are main to existing daytime cryptography. Current cryptography exists at the intersection purpose of the requests of number juggling, programming designing, electrical structure, communication knowledge, and material science. Uses of cryptography join electronic exchange, chip-based portion cards, progressed fiscal guidelines, PC PINs, and military communications. There are three types of cryptographic techniques:

1) Symmetric Key Cryptography
2) Asymmetric key cryptography
3) Hash Function Cryptography

Many solutions have been proposed however they have met with limited success. We make use of elliptical curve cryptography. Our article proposes using a secured cryptographic data model to extend the security of cloud service for next generation.

2. Literature Survey

Xiao Chun Yin proposes a plan to safely store and access of information by means of web. We have utilized ECC based PKI for endorsement system in light of the fact that the utilization of ECC essentially decreases the calculation cost, message size and transmission overhead finished RSA based PKI as 160-piece enter measure in ECC gives similar security 1024-piece enter in RSA. We have planned Secured Cloud Storage Framework (SCSF). In this system, clients not exclusively can safely store and access information in cloud yet in addition can impart information to numerous clients through the unsecure web in a secured way. This plan can guarantee the security and protection of the information in the cloud.

Tien-Ho Chen, Hsiu-lien Yeh , Wei-Kuan Shih proposed an ECC dynamic ID-Based remote shared confirmation conspire for remote gadgets to fathom the issues. Moreover, we broke down our plan to demonstrate that our plan is more secured to verify clients and remote servers for distributed computing.

Neha A Puri, Ajay R Karare ; Rajesh. C. Dharmik proposed application is conveyed on the Cloud and for the safe transmission of the information we will utilize ECC Algorithm in our task as a result of its favorable circumstances regarding CPU use, time for Encryption and Key Size. This Paper will investigate the organization of Application on the Cloud and builds the security level by actualizing ECC Algorithm, Digital Signature and Encryption.

Mill operator (1986) and Koblitz (1987) proposed an Elliptic Curve Cryptosystem (ECC) based component to give a verification system to a client can get to remote server subtly. As of late, ECC based remote verification conspire has been utilized for cloud Internet and remote gadgets. For example, Yang and Change proposed an ID-based remote shared validation with key assention conspire for remote gadgets on Elliptic Curve Cryptosystem in 2009**3.**

3. Cloud Computing Environment

3.1 CLASSIFICATION OF CLOUDS

Cloud might be characterized extensively as:

I) Public Cloud : facilitated, worked and oversaw by outsider seller from at least one server farms.

II) Private Cloud : oversaw or claimed by an association, giving administrations inside an association.

III) Hybrid Cloud : included both the private and open cloud models where association may run non - center application in an open cloud, while keeping up center applications and touchy information in-house in a private cloud.

4. Cloud Computing Entities

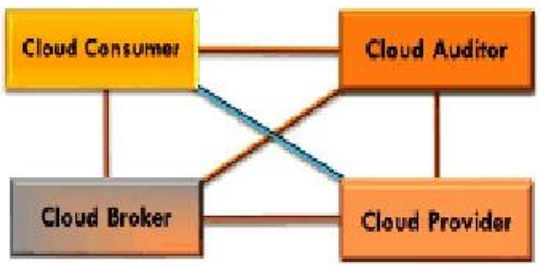

Fig:1 Cloud computing entities

- **Cloud Consumer**: One who utilizes a cloud supplier's assets, from an organization to a person.
- **Cloud Auditor**:The objective of Cloud Audit is to furnish cloud specialist co-ops with an approach to make their execution and security information promptly accessible for potential clients.
- **Cloud Broker**: the Service intermediaries focus on the transaction of the connections amongst customers and suppliers. There are two noteworthy parts for intermediaries: SLA Negotiation and VM Monitor[5]. The SLA Manager takes mind that no Service Level Agreement (SLA) is abused and VM Monitor the current expressed of virtual machines occasionally at particular measure of time.
- **Cloud Provider**: The Company who makes the cloud accessible to others

Security criteria of Server stockpiling had not been considered if there should arise an occurrence of customer server cooperation. The proposed system is Weak and less secure (as links has a tendency to be more helpless against savage power assaults). Security factors which are Randomness related, had been totally disregarded. This system isn't totally reasonable for very private information (identified with saving money, safeguard and other business related applications

5. Implementation of Elliptical Curve Cryptography in Cloud Computing

Elliptical curve cryptography (ECC) is an open key encryption method in view of Elliptical curve cryptography that can be utilized to make speedier, littler, and more effective cryptographic keys. ECC creates keys through the properties of the Elliptical curve condition rather than the customary technique for age as the result of expansive prime numbers[6]. The innovation can be utilized as a part of conjunction with most open key encryption techniques, for example, RSA, and Diffie-Hellman. As indicated by a few analysts, ECC can yield a level of security with a 164-piece key that different frameworks require a 1,024-piece key to accomplish. Since ECC sets up proportionate security with bring down registering force and battery asset utilization, it is winding up broadly utilized for versatile applications. ECC was created by Certicom, a versatile e-business security supplier, and was as of late authorized by Hifn, a producer of incorporated hardware (IC) and system security items. RSA has been building up its own rendition of ECC.

An elliptic curve isn't a circle (oval shape), however is spoken to as a circling line crossing two tomahawks (lines on a diagram used to show the situation of a point). ECC depends on properties of a specific sort of condition made from the numerical gathering (an arrangement of qualities for which tasks can be performed on any two individuals from the gathering to deliver a third part) got from focuses where the line meets the tomahawks.

Duplicating a point on the bend by a number will create another point on the bend, however it is exceptionally hard to discover what number was utilized, regardless of whether you know the first point and the outcome. Conditions in light of elliptic curvess have a trademark that is exceptionally significant for cryptography purposes: they are generally simple to perform, and amazingly hard to switch. Example of real time elliptic curve a couple of distinct logarithm-based conducts have been adjusted to elliptic curves, supplanting the gathering with an elliptic bend:

- •The elliptic curve Diffie – Hellman (ECDH) key understanding plan depends on the Diffie– Hellman plot
- •The Elliptic Curve Integrated Encryption Scheme (ECIES), otherwise called Elliptic Curve Augmented Encryption Scheme or just the Elliptic Curve Encryption Scheme
- •The Elliptic Curve Digital Signature Algorithm (ECDSA) depends on the Digital Signature Algorithm,
- •The ECMQV key assention conspire depends on the MQV key understanding plan.

- •The ECQV certain authentication plot**.**

6. Research Model

The underlying level of security display is involved into 3 noteworthy parts. The proposed system is:

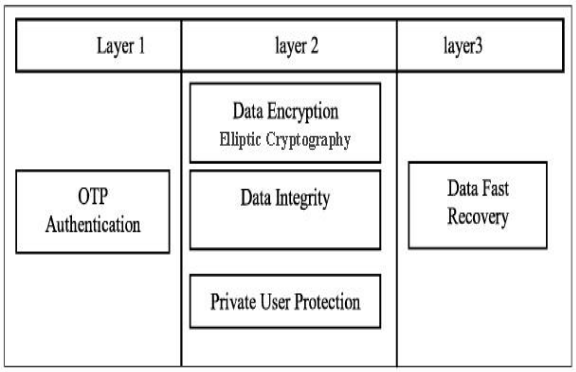

Fig:2 Proposed model using ECC

STAGE 1:
OTP Authentication
STAGE 2:
It is subdived into three parts:

- Data Encryption
- Data integrity
- Private User Protection

STAGE 3:
Data fast recovery
STAGE 1:
OTP Authentication:

To start with level of security is a secured OTP stick, where the remote host gets the secret key for each login to the registered mobile number or mail id of the user. Here in our model 6places are designated for OTP with size of 40 bits(8 bits for two integer values and 32 bits for four characters in which 16 bits for upper case and another 16 bits for lower case characters)[11] .The OTP is given a 30 seconds duration of lifetime. If the OTP has not been entered by the user then that OTP will be expired and the user have to send request to generate new OTP for login.
STAGE 2:

The second stage can be divided into .i) Data encryption using ECC, ii) Data integrity, iii) Private user protection.

I)Data Encryption using ECC:

The first level of the second stage includes with Crypto graphical security demonstrate utilizing Elliptic bend cryptography which is coordinated alongside the SSL burrow and each host is scrambled with 256 piece key utilizing ECC. Information honesty of each host is checked remotely by means of transmission and the document exchange is expert by implies secured burrow. Different security arrangements are recorded as convention and connected amid on-request information handling. In the existing system RSA keys are used for data encryption and the recommended size of these keys keep increasing(example from 1024 bits to 2048 bits some years ago) for sufficient cryptographic strength[12]. So instead of RSA we use ECC keys where both the keys share same important property of asymmetric algorithm (one for encryption and one for decryption).
We are replacing RSA keys with ECC keys because ECC can provide same cryptographic strength as RSA system with much smaller key sizes (For instance 160 bits in ECC is identical to 1024 bits in RSA key). The small key sizes make ECC extremely engaging for gadgets with restricted capacity or handling power, which are winding up progressively normal in the IoT. As far as more conventional web server utilize cases, the littler key sizes can offer speedier SSL handshakes (which can mean quicker page stack times) and more grounded security. Hence we use ECC keys in our model.

II)Data Integrity:

The second level of second stage comprises of data integrity. Information honesty is a basic segment of data integrity. In its broadest utilize, "data integrity" alludes to the exactness and consistency of information put away in a database. The term – Data Integrity - can be utilized to portray an express, a procedure or a capacity – and is frequently utilized as an intermediary for "information quality". Information with "trustworthiness" is said to have an entire or entire structure [7]. Hence here an authentication should be given (example: mobile number, mail id, etc.) to identity whether the user is trying to login or some third parties is trying to access the user's account.

Types of Data Integrity

Three types of data integrity are as follow: referential integrity, entity integrity and domain integrity:

Entity Integrity: It concerns the possibility of a fundamental key. Substance uprightness is a dependability choose which communicates that each table must have a fundamental key and that the portion or sections been the basic key should be excellent and not invalid.
Referential Integrity: It concerns the possibility of a remote key. The referential respectability choose states that any remote key regard must be in one of two states[8]. The standard circumstance is that the outside key regard insinuates a basic key estimation of some table in the database. Now and again, and this will depend upon the rules of the data proprietor, a remote key regard can be invalid.
Domain Integrity: It demonstrates that all segments in a social database must be declared upon a portrayed territory. The fundamental unit of data in the social data demonstrate is the data thing. Such data things are said to be non-decomposable or atomic. A zone is a game plan of estimations of a comparative sort.

III)Private User Protection:

The third level of the second stage includes private user protection. In RSA together the dispatcher and receiver are provided with the identical key (public key) by which the third parties can access the data during transmission whereas in ECC the sender and receiver are provided with two different keys public key and private key. The dispatcher will have public key and when the information is sent to receiver the receiver uses his/her own private key to open the encrypted information. Hence no third party can access the information during the transmission since two keys are used.

STAGE 3:
Fast Recovery Data:
Third stage of model is went with to recuperation arrangement which recoups the commotion information and ping back to the prior stages. The small key sizes make ECC very appealing for devices with limited storage or processing power, which lets the user to fast data recovery.

ADVANTAGES:

1) Remote host information can't saw by MITM host's.
2) No question based infusion
3) SQL switch isn't conceivable
4) Brute constraining and other crypto graphical strategies can't be connected to unscramble the information grouping.
5) Peer – peer, server - server record sharing is done remotely utilizing secured burrow

7. Conclusion

Cloud computing is one of the present most sultry research regions because of its capacity to decrease costs related with programming and data are given to purchasers on request progressively. Since, Cloud computing share scattered assets by means of the system in the open condition; henceforth it makes security issues indispensable for one to build up the Cloud computing applications. Consequently we proposed an ideal ECC based cloud crypto graphical security model to give security amid remote host record transmission. The proposed is having high viability as far as demonstrating security due its 256 piece encryption.

8. References

[1] P. Mell and T. Grance, "Recommendations of the National Institute of Standards and Technology", 2011, National institute of Standards and Technology, US Department of Commerce

[2] Peeyush Mathur and Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 1st International Conference on Parallel, Distributed and Grid Computing

[3] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, "NIST Cloud Computing Reference Architecture", 2011

[4] W Stallings, "Cryptography and Network Security: Principles and Practices", pp. 420-430, 2009, Prentice Hall

[5] D Hankerson, A Menezes and S Vanstone, "Guide to elliptic curve cryptography", 2004, Springer-Verlag

[6] N Koblitz, "Elliptic Curve Cryptosystem", Journal of mathematics computation, vol. 48, no. 177, pp. 203-209,

[7] Antony Kumar K, Manikandan N.K, Manivannan D "Analysing performance metrics for data centric protocol in Wireless Sensor Networks ", International Journal of Applied Engineering Research, May-2015. Vol: 10, Issue: 8, PP 19819-19827.

[8] V Miller, "Use of elliptic curves in cryptography", Proc. of Advances in Cryptology-CRYPTO, 85, vol. 218, pp. 417-426

[9] V. Miller, "Uses of elliptic curves in cryptography" in Lecture Notes in Computer Science 218: Advances in Cryptology-CRYPTO, vol. 85, pp. 417-426, 1986, Springer-Verla

[10] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209, 1987

[11] Antony Kumar K, Manikandan N.K, Manivannan D, Saran Raj S, "A novel security mechanism for IEEE 802.11i", International Journal of Applied Engineering Research, Mar-2015. Vol: 10, issue: 3, pp- 6745-6754.

[12] C. C. Lee, M. S. Hwang and W. P. Yang, "Extension of authentication protocol for GSM", vol. 150, no. 2, 2003, IEEE

[13] Ray Sangram and G. P. Biswas, "An ECC based public key infrastructure usable for mobile applications", Proceedings of the Second International Conference on Computational Science Engineering and Information Technology-CCSEIT 12

[14] Rashmi , Ramesh Chavan and Manoj Sabnees, "Secured mobile messaging", 2012 International Conference on Computing Electronics and Electrical Technologies (ICCEET).

a. S. Durai , N. Rajkumar, N. K. Manikandan and D. Manivannan "Data Entry Works in computer using Voice Keyboard", Indian Journal of Science and Technology, Vol 9(2), DOI:10.17485/ijst/2016/v9i2/85814, January 2016

cessing while at the same time expanding adaptability and adaptability for figuring administrations. Cloud computing is web centered registering because of shared assets,