International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 09 | Sep -2017 www.irjet.net p-ISSN: 2395-0072

Cloud Data Security Using Elliptic Curve Cryptography

Arockia Panimalar.S [1], Dharani.N[2], Pavithra.S[3], Aiswarya.R[4]

[1] *Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India*
[2,3,4] *III BCA, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India*

Abstract - *Data security is, protecting data from ill-conceived get to, utilize, introduction, intrusion, change, examination, recording or destruction. Cloud computing is a sort of Internet-based computing that grants conjoint PC handling resources and information to PCs what's more, different gadgets according to necessity. It is a model that empowers universal, on-request access to a mutual pool of configurable computing resources. At present, security has been viewed as one of the best issues in the improvement of Cloud Computing. The key issue in effective execution of Cloud Computing is to adequately deal with the security in the cloud applications. This paper talks about the part of cryptography in cloud computing to improve the data security. The expectation here is to get bits of knowledge another security approach with the usage of cryptography to secure information at cloud data centers.*

Key Words: **Cloud Computing, Elliptical Curve Cryptography, Cryptography**

1. INTRODUCTION

Cloud computing provides a new way of services by organizing various resources and providing them to users based on their demands. It also plays a crucial role in the next generation mobile networks and services (5G) and Cyber-Physical and Social Computing (CPSC). Cloud computing and capacity arrangements give clients and ventures different qualities to store and process their information in third-party data centers that might be arranged a long way from the user running in remove from over a city to over the world. Cloud computing counts on sharing of resources to attain endurance and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Storing data in the cloud greatly decreases storage load of users and brings them access comfort, thus it has become one of the most important cloud services. Possibilities guarantee that, cloud computing enables organizations to keep away from forthright infrastructure costs (e.g. purchasing servers). Likewise, it engages associations to focus on their core businesses instead of investing energy and supports on computer infrastructure. Cloud computing enables undertakings to get their applications up and running speedier, with enhanced sensibility and less maintenance. Be that as it may, concerns are starting to create about how safe Cloud is? as more data on people and organizations are being put in the cloud. Disregards to all the hype surrounding the cloud, enterprise customers are still unwilling to place their business in the cloud. One of the real concerns which lessens the development of Cloud computing is security and impediment with data security and information protection keep on infecting the market. Cloud information storage augments the danger of data spillage and ill-conceived get to. The architecture of cloud poses certain dangers to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be alert in interpreting the risks of data intrusion in this new environment.[1] The security concerns with respect to cloud computing are end-user data security, network traffic, file systems and host machine security which can be addressed with the help of cryptography to a considerable level. "Security and privacy are indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security."[2]

What is Cryptography?

Cryptography is the art and science of assuring security by converting information messages into non- readable ones. The original message also referred to as plain text message is in simple English language that can be interpreted by everyone.

The encrypted message, obtained by applying cryptographic techniques to the plain text, is called as cipher text message. There are three types of cryptographic techniques:

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

2. LITERATURE SURVEY

1.Wang, L., Tao, J., & Kunze, M. in their research paper "Scientific cloud computing: Early definition and experience" says that, Computing clouds equips users with services to access hardware, software, and data resource. Some clouds service models are:

i) HaaS: Hardware as a Service

Hardware as a Service was proposed possibly at 2006. As an outgrowth of rapid advances in hardware virtualization, IT automation and usage metering and pricing, users could buy IT hardware - or even an entire data center/computer center

- as a pay-as-you-go subscription service. The HaaS could be flexible, scalable and manageable to meet your needs.

ii) SaaS: Software as a Service

Software or application is hosted as a service and provided to customers across the Internet, which excludes the requirement to install and run the application on the customer's local computer. SaaS therefore amends the customer's headache of software maintenance, and decreases the expense of software purchases by on demand pricing.

iii) DaaS: Data as a Service

Data in various formats, from various sources, could be accessed via services to users on the network. Clients could, for instance, control remote information simply like work on local disk or access data semantically on the Internet.

2. Er. Sharanjit Singh and Er. Rasneet Kaur Chauhan, "Introduction to CryptoCloud in Cloud Computing"proposes Cryptographic Algorithms as:

1) Data Encryption Standards (DES)
2) Advanced Encryption Standards (AES)
3) Triple – DES
4) RSA
5) Blowfish

These algorithms can be applied successfully in cloud environment.

3. Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, Mats Näslundy and Makan Pourzandi in their research paper, "An quantitative analysis of current security concerns and solutions for cloud computing" says that aiming to organize the information related to cloud security have identify the main problems in the area and grouped them into a model composed of eight categories: Compliance, Trust, Architecture, Identity and Access, availability, incident response, data protection and governance.

Fig.1: Security Problems in Cloud Computing Environment

3. CLOUD COMPUTING ENVIRONMENT

A) History and Definition

Cloud computing bursts as a hot topic from the late of 2007 due to its capabilities of rendering elastic propelling IT infrastructures, QoS assured computing environments and configurable software services [3]. The Cloud Computing provides computing over the internet and this word is basically inspired by the weather cloud. In cloud, data is stored at remote location and is available on demand. It allows clients to use application software without installing the file at any computer locally, with internet connectivity. By data outsourcing user can obtain the required information from anywhere more efficiently and has no headache of storage space and can skip the extra expenses on software, hardware, and information resources and data maintenance [2].

B) Current Cloud Projects

Currently numerous projects from industry and academia have been proposed, for example, RESERVOIR project [4] - IBM and European Union joint research initiative for Cloud computing, Amazon Elastic Compute Cloud [5], IBM's Blue Cloud[6], scientific Cloud projects such as Nimbus [7] and Stratus[8], OpenNEbula [9].

C) Classification of Clouds

Clouds may be classified broadly as:

i) Public Cloud: hosted, operated and managed by third party vendor from one or more data centers.
ii) Private Cloud: managed or owned by an organization, providing services within an organization.
iii) Hybrid Cloud: comprised both the private and public cloud models where organization might run non - core application in a public cloud, while maintaining core applications and sensitive data in- house in a private cloud.

D) Features of Cloud Computing

i) Resource Pooling and Elasticity

In cloud computing, resources are pooled to serve a large number of customers. Cloud computing utilizes multi-tenure where distinctive resources are progressively allotted and de-assigned by request. From the client's end, it is unrealistic to know where the resource really resides. The resource allocation ought to be flexible, as in it should change suitably and rapidly with the demand. In the event that on a specific day the request expands a few times, at that point the system ought to be sufficiently versatile to meet that extra require, and should come back to the normal level when the demand diminishes.

ii) Self and On-Demand Service

Cloud computing depends on self-service and on-demand service models. It ought to enable the client to collaborate with the cloud to perform assignments like building, deploying, managing, and scheduling. The client ought to have the capacity to get to figuring abilities as and when they are required and with no association from the cloud service provider. This would help clients to be in control, getting deftness their work, and to settle on better choices on the present and future needs.

iii) Broad Network Access

Capabilities are accessible over the network and got to through standard mechanisms that advance use by heterogeneous thin or thick client stages (e.g., cell phones, tablets, portable PCs and workstations).

iv) Measured Services

Cloud systems consequently control what's more, upgrade resource use by utilizing a metering ability at some level of reflection proper to the type of service (e.g. storage capacity, processing, transmission capacity and active client accounts). Resource utilization can be monitored, controlled and reported, giving straightforwardness to the provider and consumer.

v) Rapid Flexibility

Capabilities can be flexibly provisioned and discharged, now and again naturally, proportional quickly outward and internal proportionate with demand. To the customer, the capacities accessible for provisioning regularly have all the earmarks of being boundless and can be appropriated in any quantity whenever.

E) Cloud Computing Entities

Figure shows the cloud computing entities:

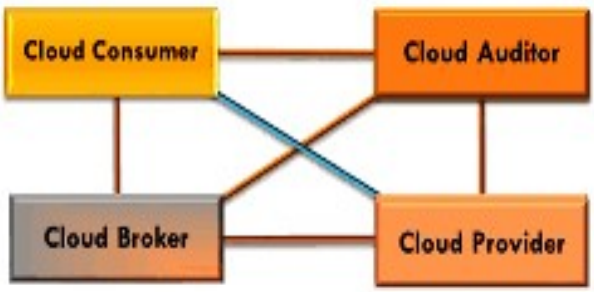

Fig: Cloud Computing Entities

i) Cloud Consumer: One who uses a cloud provider's resources, from a company to an individual.
ii) Cloud Auditor: The goal of Cloud Audit is to provide cloud service providers with a way to make their performance and security data readily available for potential customers.
iii) Cloud Broker: the Service brokers concentrate on the negotiation of the relationships between consumers and providers. There are two major roles for brokers: SLA Negotiation and VM Monitor. The SLA Manager takes care that no Service Level Agreement (SLA) is violated and VM Monitor the current stated of virtual machines periodically at specific amount of time[2].
iv) Cloud Provider: The Company who makes the cloud available to others. They are in charge of maintenance/ upkeep of the cloud and, of course, making sure it is always available to the cloud user.

4. ROLE OF CRYPTOGRAPHY IN CLOUD COMPUTING

A) Introduction to Cryptography

Cryptography is the technique widely used in computer networks to provide security to the data and messages communicated over the network. The plain text message being sent from sender is encrypted in to a special format called as "Cipher Text" by applying some cryptographic algorithm and then communicated over the network. At the receiver's end, the Cipher text message is decrypted in the original plain text again by applying some decryption algorithm. Thus only the sender & receiver of the communication can read the encoded message and no one else. Cryptography is used for addressing the network security problems.

i. Data Integrity: Information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
ii.Authentication: Determining whom we are talking to before revealing the sensitive information or entering into a business deal.
iii. Non Repudiation: Deals with signatures and is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
iv. Secrecy: Keeping information out of the hands of unauthorized users, relates to loss of privacy, identity theft.

B. Cryptographic Model

The following figure helps to understand the basic idea of cryptography.

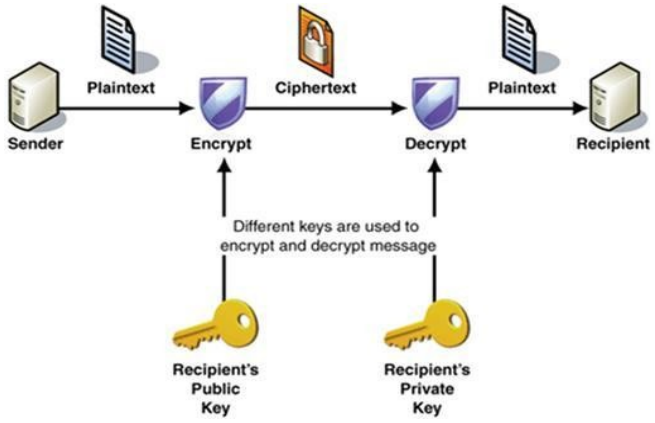

Fig: Cryptographic Model

i) Plaintext is the original source information or data that is input to algorithms.
ii) Cipher text is the scrambled message output as random stream of unintelligible data.
iii) Encryption Algorithm substitutes and performs permutations on plain text to cipher text.
iv) Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
v) Keys are used as input for encryption or decryption and determines the transformation.
vi) Sender and Recipient are persons who are communicating and sharing the plaintext.

C) Classification of Security Algorithms

i) Private Key/ Symmetric Algorithms: These algorithms use a single secret key that is known to the sender and receiver.
E.g. RC6, AES, 3DES, IDEA, Blowfish.
ii) Public Key/ Asymmetric Algorithms: Use a key pair for cryptographic process, with public key for encryption and private key for decryption
E.g. RSA, Diffie Hellman

D) Security Issues that arise in the Cloud

Security issues in cloud fall into two general classes: security issues confronted by cloud providers (associations giving programming, platform, or framework as-a-benefit by means of the cloud) and security issues confronted by their clients (organizations or associations who have applications or store data on the cloud)[15].

i) Guaranteeing Data isolation
In order to optimize resources, cut costs, and maintain efficiency, Cloud Service Providers store multiple customers' data on the same server. This leads to a chance that user's private data can be viewed by each other. To avoid such sensitive situations, cloud service providers must ensure proper data isolation and logical storage separation.

ii) Guaranteeing Secure Data Transfer
In a Cloud environment, the physical location and reach are out of control of the end user, where the resources are hosted.
iii) Ensuring Secure Interface
In the unsecure internet environment the integrity of information during transfer, storage and retrieval needs to be ensured.
iv) Security of Stored Data
The issue of controlling the encryption and decryption by either the end user or the Cloud Service provider is still doubtful.
v) User Access Control
Web data logs are needed to be provided to compliance auditors and security managers for web based transactions (PCI DSS).

In the referenced research work, a security framework has been proposed for cloud computing to assure confidentiality, integrity and authentication criteria using symmetric and asymmetric cryptographic algorithms. But there are still some problem areas observed in this work listed as follows[10]:

->No any strong valid authentication scheme had been proposed or implemented yet.
->Security criteria of Server storage had not been considered in case of client-server interaction.
->The proposed framework is Weak and less secure (as concatenations tends to be more vulnerable to brute-force attacks).
-> Security factors which are Randomness related, had been completely neglected.
->This framework is not completely suitable for highly confidential data (related to banking, defense and other brokerage related applications).

5. Elliptical Curve Cryptography in Cloud Computing

Elliptic Curve Cryptography (ECC) is effectively used as a touch of preparing to instantiate public key cryptography conventions, for instance executing keys and digital signatures. There are diverse motivations behind energy of using elliptic bends as they offer more little key sizes and more possible executions [11].

ECC is a kind of open cryptosystem like RSA. Be that as it may, its snappier advancing limit and by giving appealing and option approach to specialists of cryptographic calculation influences it to contrast from RSA. A similar security level gave by RSA, can be additionally given by ECC, that likewise with littler key sizes. For example, the 1024 bit security strength of a RSA could be reduced to 163 bit security strength of ECC with the same level. Apart from this, ECC is especially well suited for wireless communications, like mobile phones, PDAs, smart cards and sensor networks.

ECC uses point of multiplication operation, which has been found to be computationally more efficient than RSA exponentiation[12].

ECC has drawn much attention as the security solutions for wireless networks such as Clouds, due to the small key size and simplified computation [13]. Elliptic curve has a unique property that makes it fit for use in cryptography in cloud computing i.e. its power to take any two points on a specific curve, add them together and get a third point on the same curve. The fundamental operation engaged with ECC is point multiplication, i.e. increase of a scalar K with any guide P on the curve toward get another point Q on the same curve[14]. The general equation for an elliptic curve is:

$$y2 + axy + by = x3 + cx2 + dx + e$$

Where a, b, c, d and e are real numbers and x and y belongs to a set of real number. In its simplest form, an elliptic curve equation can be given as:

$$y2 – x8 + dx + e$$

6. ANALYSIS

A Statistical investigation, demonstrates that a similar level of security rendered by a RSA-based framework with a huge modulus can be proficient with a considerably smaller elliptic curve group, i.e. a 163 piece key of ECC is thought to be as secure as 1024 bits key in RSA. Also ECC uses smaller key sizes, which effects in faster calculations, lower power consumptions, saving memory and bandwidth. ECC thus clubbed with Cloud computing will definitely provide much more secure environment along with speed and saving of many intangible/indirect resources. ECC applied in cloud will result in more attention paid towards how to avoid data duplications, how to utilize data and services efficiently and how to achieve cost-effective solutions.

7. CONCLUSION AND FUTURE ENHANCEMENT

Cloud Computing is utilized for service-based architecture. To plough on cloud computing, the community must take sincere and dedicated measures to ensure security. A movement continues to adopt universal standards (for example, open source) to ensure interoperability among service providers.

ECC can be utilized as a part of mobile computing, remote sensor systems, server based encryption, image encryption and its application in each field of communication. Cloud computing with ECC is a totally new area and has colossal extent of research. The concern here is data security with Elliptic curve cryptography to give secrecy and confirmation of data between clouds. In future, security issues of cloud computing can be focused more and an attempt can be made to discover better solutions utilizing Elliptical Curve Cryptography.

8. REFERENCES

[1]S. Subashini, V. Kavitha -Anna University Tirunelveli, India," A survey on security issues in service delivery models of cloud computing"ELSEVIER- Journal of Network and Computer Applications Volume 34, Issue 1, January 2011, Pages 1–11.

[2] Jashanpreet Pal Kaur, Rajbhupinder kaur, Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab, "Security Issues and Use of Cryptography in Cloud Computing"

[3] Wang, L., Tao, J., & Kunze, M. (2008). "Scientific cloud computing: Early definition and experience".

[4] Reservoir Project [URL]. http://www-03.ibm.com/ press/us/en/pressrelease/23448.wss/,access on June 2008.

[5] Amazon Elastic Compute Cloud [URL]. http://aws. amazon. com/ ec2, access on Nov. 2007.

[6] IBM Blue Cloud project [URL]. http://www-3.ibm.com/press /us/en/pressrelease/22613.wss/, access on June 2008.

[7] Nimbus Project [URL].http://workspace.globus.org/ clouds/nimbus.html/,access on June 2008.

[8] Status Project [URL]. http://www.acis.ufl.edu/vws/, access on June 2008.

[9] OpenNEbula Project [URL].http://www.opennebula.org /, access on Apr.2008.

[10] Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.

[11] Shweta Sharma, Bharat Bhushan, Shalini Sharma - "Improvising Information Security in Cloud Computing Environment"- International Journal of Computer Applications (0975 – 8887) Volume 86 – No 16, January 2014.

[11]D. J. Bernstein and T. Lange (editors). eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench. crypto, October 2013.

[12] Dr.R.Shanmugalakshmi, M.Prabu – "Research Issues on Elliptic Curve Cryptography and Its applications"- IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[13] Wang, H., Sheng, B. and Li, Q. (2006) 'Elliptic curve cryptographybased access control in sensor networks', Int. J. Security and Networks,Vol. 1, Nos. 3/4, pp.127–137.

[14] Ms Bhavana Sharma, B.P.I.T., Rohini, Delhi-"security architecture of cloud computing based on elliptic curve cryptography (ecc)" ICETEM 2013.

[15] Wikipedia, the free encyclopedia of Cloud Computing.

[16] Khanna, D. (2019). Internet of Things Challenges and Opportunities. International Journal For Technological Research In Engineering