Securing Data Storage by Virtualization in Cloud using Cryptography Protocols

Nuthakki praveena[1], k.madhavi[2], Geetha. G[3]

[12 3]*Assistant professor & Department of IT & VR Siddhartha Engineering College, Vijayawada, India*

Abstract: *Cloud storage is quickly turning into a green pasture to speculate certain trendy organizations. It provides the user tons of flexibility with the event of varied applications with the design and additionally offers varied price/value and different advantages to the organization. Though cloud computing is gaining quality for its low price of operations and simple implementations and use, one has to be compelled to take care of a number of the protection aspects cherish information loss, privacy, cyber-attacks, and unauthorized access. This paper suggests building a security framework specific to a cloud-based atmosphere by which organizations will manage the safety of their information and protect it from attack, by providing the information with confidentiality and integrity using Elliptic Curve Cryptography.*

Keywords:-*cloud computing, confidentiality, Integrity, Cyber-attacks, Elliptic curve cryptography.*

I. INTRODUCTION

The definition of cloud computing is defined as "A model for acquiescence opportune, dynamic network access to a common pool of configurable computing resources (e.g, networks, servers, storage, applications and services) that may be speedily provisioned and released with minimal management effort or service provider interaction" by The National Institute of Standards and Technology , a part of the United States, Department of Commerce [1].Cloud computing is changing the standards of the IT amusement. The cloud technology is clearing crosswise over business segments and changing the way organizations work together [2]. In addition the way clients access information, administrations, and applications. When you store your information in distant storage locations like mails and websites instead of your local storage, specifies that you are utilizing a "Cloud Computing" service. For example consider an associate using an in-house invoicing service from a very long time wants to upgrade to online invoicing service is one of the cloud computing services [3]. Cloud computing isolates data and implies the transport of figuring resources over the network and updates applications for your prerequisites. Cloud users can access these applications over the internet in any location. Instead of keeping centralized data centre, IT departments focus on the strategic project [2].

Cloud Layers

Even though cloud computing is getting more popularity it is important to understand the service layers that define it. In cloud computing each layer in the model exists conceptually on the foundation of the previous layer

Client: A cloud customer comprises of equipment and/or PC programming bundle that relies on upon distributed computing for application conveyance which is basically futile without it. Example embraces some computer (Chrome book), Phone (Google Nexus) and different devices.

Application: Software as a service one of the cloud computing services delivers software packages over the network eliminating the overhead of installing, maintaining at users local computer and thus providing a flexible way to cloud users of running applications at their computers [4]. Cloud having software as a service maintains package of interconnected tasks, the definition of those tasks, and also the configuration files, that contain run time information of the tasks.

Platform: Delivers a computing platform and can also be called as plat form as a service [4].It is like stack as a service. In general it plays a key role to provide a cloud infrastructure and also supports cloud applications. It is easy to buy and manage underlying hardware and software package layers without any price and can also facilitate preparation of applications.

Infrastructure: Cloud provides computer infrastructures to its users under its service called as "Infrastructure as a Service" [4] which provides raw (block) storage and networking instead of buying servers, software, data-centre area or network equipment to clients as a totally outsourced service.

Advantages of Cloud Computing:

Some of the advantages of cloud computing is given below Organizations can pay incrementally to the used cloud services thereby saving their wealth.

- Organizations can have more storage area than on their personal systems.

- IT personnel need not worry for maintaining their software packages up to date.
- Cloud computing is more flexible and reliable when compared to past computing ways.
- Users need not be at their desks and can access their data from any location
- Cloud users need not worry regarding consistent computer hardware updates and different computing problems,
- Organizations can concentrate on core activities.

Cloud Data Security:

A new tumultuous technology[5] similar to cloud computing comes with its associated risks, where as a number of these risks are like those within the traditions service provision model, others are distinctive to cloud computing, and information security is vital in any respect levels of cloud computing atmosphere. The users should make sure that any sensitive or regulated information isn't placed about what information the provider collects which way it's protected; like how metadata is secured, what access customers have to do that metadata, what security controls provided are enforced at the network level and then on. The Major areas where information security can be in danger and with to be alleviated are as follows:

Cloud data-in-transit: The protocol uses to transfer data across clouds provides confidentiality and integrity that's the information transfer happen in the encrypted channel.

Cloud data-in-rest: It's powerfully suggested to encode the data-at-rest in iaas, paas and saas cloud for easy storage only.

Processing of Data: Information must be encrypted when it is processed within the cloud, which implies that it permits the information to be processed while not decoding.

Data Lineage: Following the path data (mapping application information flows or information path visualization) is understood as information lineage that's precisely once and wherever the information was specifically situated inside the cloud and maintained for auditor's assurance.

Data Provenance: Information provenance means not only information has integrity, but it is also computationally accurate.

II. State of Art:

The related work regarding security and integrity problem and projected protocols have mentioned in this paper. A solution has been proposed in [6, 7] for remote data integrity that uses RSA functions to hash the entire record. Another approach proposed by [8] that addresses several challenges where the server stores the data, sends a MAC address as a response to the challenge message. A protocol is proposed in [9] to verify the distant information in which infinite number of verifications is required and at set time running time can be chosen. Proposed a privacy-preserving audit protocol, that permits a third party auditor to stay online storage honest [10, 11]. A protocol which is more secured has been proposed in [12] to validate the self-organizing storage periodically.

An efficient way is proposed to perform periodical integrity of information while not having the native copy of information files as in 13, 14]. A more deterministic solution has been proposed in [15] to moderate the security drawback issues that exist in cloud. Two drawbacks in [16] are one is mismatch between the stored and computed values of checksums and the other is computed values from one way hash functions. They proposed a replication and demonstrable possession information over cloud servers with dynamic data support as in [17]. An efficient remote information possession is projected in [18] which have the advantages like computation, communication and also permits verification without the necessity for the challenge to check against the first data. A scheme proposed in [19] achieves availability and integrity of the information store in cloud, but drawback is it does not address confidentiality.

Table 1: Authors and papers Details description

Author	Title	Description
"SabahiFarzad" in the year 2011	"The cloud computing security threats and responses"	Using access control managements they addresses issues like reliability ,availability and security in cloud computing
"Xiang Tan Bo Ai" in the year 2011	"The issue of cloud computing security in high-speed Railway"	To resolve the traffic and monitor the VM ,they developed the virtual firewall
"Govinda V and Gurunathaprasad H Sathshkumar" in the year 2012	"Thirdparty auditing for secure data storage in cloud through Digital Signature using RSA"	Using private and public keys in RSA algorithm, Third party encrypted the data and store in the cloud.
"Ravi Kant Sahu,AbhishekMohta and L.K Awasthi" in the year	"Robust data integration while using TPA for Cloud Data Storage Services"	Third party uses AES encryption algorithm to store the data

As described in the table, all authors proposed different types of methods using different algorithms to encrypt the data, but they fail to implement security of data efficiently. The main drawback of these schemes is, they do not involve in the privacy protection of the data. This paper provides an efficient and secure to keep the could data more secured.

III. Proposed Security Solutions

Cryptography is more familiar and extensively used technique that manipulates data to cipher or hide their existence accordingly. In cryptography, encryption is the technique of coding the data/information in such the way that solely approved parties will read it. In an encryption scheme, the data/information, mentioned in plaintext, is encrypted using a coding algorithmic rule, turning it into an unreadable text. This can be sometimes done with the use of any encryption key that specify how the information is to be converted to unreadable format. Any opponent who sees the cipher text shouldn't be ready to make out anything regarding the initial message. A trusted person, however, is ready to decode the encoded text using a decryption algorithm that usually needs a undisclosed decoding key that rival don't have access to. For security reasons, an encryption scheme sometimes desires a key-generating algorithmic program to at random produce keys.

This paper tends to propose a well-organized and way better protected protocol than previous protocols to ensure the secrecy and reliability of information hosted in aloud using Elliptic Curve Cryptography (ECC).

IV Architecture Model

Fig 1: Architecture for securing Cloud Data

In the Fig1 it is clear that how the data is storing in the cloud and how it can be accessed by the authorized users and also how the action can be performed for securing the information against the attacks is represented. The types of attacks were explained in brief:

There are two types of threats: A threat can be occurred due to some malicious parties. They tend to gain the information by using hacking systems and two of those threats are explained as follows .

Internal Threats: These threats depend up on the loyalty of the service provider and usually caused internally within the cloud where the administrator leaks the data of the user or modify it for his own purpose [20].

External Threats: These are caused by third parties who can access the information and use it for wrong intentions, or leak or modify and delete the information to meet his own needs [20].

Fig 2: Diagram representing the Attacks

Fig2 Represents the attacks that have been occurred because of the malicious third parties and these may be overcome with an efficient and secure technique projected during this paper.

This security challenge is addressed by this method. To solve this problem information is distributed into several fractions in spite of the repository of the initial data and this can be achieved through Elliptical Curve Methodology. This solution is composed of integrity, and confidentiality are also extremely adept and much better than those pseudorandom sequences.

V Cloud Security Implementation

Once information is stored in a cloud, there might be certain issues regarding privacy, compliance and governance. Privacy issues embody queries of security and whether or not your competition or malicious users will access sensitive company or client information [21]. If confidential information is be consumed or accessed by individuals outside the organizations, it's vulnerable to information fraud and different complications, like ancient IT service suppliers, enterprises expect cloud service providers (CSPs) to verify their tight security audits and certifications. Compliance is the very important feature of security. Enterprises ought to let the CSPs recognize the parameters they'll be evaluated and audited against. The providers ought to even control responsible by regulative agencies to confirm compliance with the foremost tight controls and measure. Governance may be a key challenge. Enterprises worry concerning information possession and what privileges (such as access, update and delete and delete) users might have once process their information [22] totally different deployment models present different governance problems. It's essential that enterprises perceive these problems related to a cloud preparation so as to effectively manage the safety of their data. Enterprises need to judge the security of their information and also the effectiveness of their security measures against cyber-attacks. Company and client information security are a very important

consideration regardless of whether or not the info is maintained by the company itself or by the third party Cloud Service Providers. It's vital to observe the protection and also the numerous steps taken by the provider to shield the info from cyber as well as natural attacks [23].

Elliptical Curve Cryptography: ECC is method that deals with open key cryptography and depends on the hypothesis of elliptic curve. Elliptic curve were proposed for the utilization as the premise for discrete logarithm based cryptosystems. The elliptic curve doesn't have any connection to ellipses, though the condition for oval is a quadratic condition the elliptic curve then again are cubic bends. The elliptic curves are called elliptic as a result of their relationship to elliptic essential in mathematics.

The arrangement of focuses on an elliptic bend with coordinates in relative field likewise shape a gathering and the operations is as per the following: To include two focuses P (XP, YP) and Q (XQ, YQ) on the bend pass a straight line through them and search for the third purpose of convergence with the bend, R(XR, YR). Such that P+Q= - R where –R is the impression of point R over the X – pivot. The three focuses P, Q and R lie on a typical straight line, and the focuses that shape the crossing point of a capacity with the bend are considered to indicate zero.

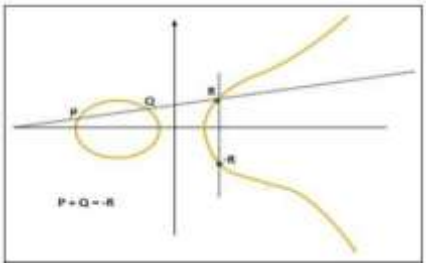

Fig 3: Linear graph representing points in sequence

In Fig 3 it is representing that three points which are plotted in the graph are in the sequential way,due to this reason intersection of the points may not be occur, so that the path is Secure. An ECC equation is as follows:

S = (YP-YQ)/(XP-XQ)

Where S is the slope of the line through P and Q

XP-S2-XP-XQ

YR = -YP+S(XP-XR)

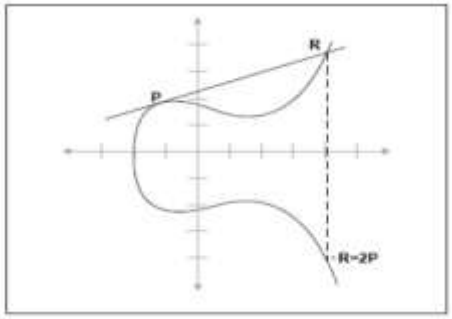

Fig 4: Representing Curve

In the above Fig 4, the points are plotted all together so that, the diagram has come fit as a fiddle. A portion of the conditions are as per the following: If XP = XQ and YP = YQ then

XR = S2-2XP

YR = -YP + S(XP-XR)

If XP = XQ and YP = YQ then R = 0 and if either point is 0 then the result is the other point. If P = Q, then the cords reduce to the tangent. The result of the operation is associate, commutative and distributive.

Proposed Algorithm for Data Security using ECC

Both clouds consent to some freely known information thing.

a.The elliptic bend condition, estimations of a and b, prime,p

b.The elliptic gathering registered from the elliptic bend condition

c.A base point, B, taken from the elliptic gathering

Key generation:

1.A chooses a whole number dA. This is A's private key.

2.A then creates an open key PA=dA*B 3. B comparably chooses a private key dB and registers an open key PB= dB *B 4. A creates the security key K= dA *PB. B creates the discharge key K= dB *PA.

Signature Generation:

For marking a message m by sender of cloud A n, utilizing

A's private key dA

1. Ascertain e=HASH (m), where HASH is a cryptographic hash capacity, for example, SHA-1 2. Select an irregular number k from [1, n - 1]

3.Ascertain r = x1 (mod n), where (x1, y1) = k * B. On the off chance that r = 0, go to step 2

4. Ascertain s = k - 1(e + dAr)(mod n). On the off chance that s = 0, go to step 2

5. The mark is the pair (c, l)

6. Send signature (c, l) to B cloud.

Encryption algorithm:

Assume A needs to send to B a scrambled message.

1. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic gathering.

2. A picks another irregular whole number, k from the interim [1, p-1]

3. The figure content is a couple of focuses PC = [(kB), (PM + kPB)] 4. Send ciphertext PC to cloud B.

Decryption algorithm:

Cloud B will find a way to unscramble figure content PC.

1. B figures the result of the principal point from PC and his private key, dB * (kB)

2. B then takes this item and subtracts it from the second point from PC (PM + kPB) – [dB(kB)] = PM + k(dBB)
– dB(kB) = PM
3. B cloud then translates PM to get the message, Msg.

Signature Verification:

For B to authenticate A's signature, B must have A's public key PA

1. Verify that c and l are integers in [1, n − 1]. If not, the signature is invalid
2. Calculate e = HASH (msg), where HASH is the same function used in the signature generation
3. Calculate w = l −1 (mod n)
4. Calculate u1 = ew (mod n) and u2 = rw (mod n)
5. CalcUlate (x1, y1) = u1B + u2PA
6. The signature is valid if x1 = c(mod n), invalid otherwise.

Results

The results that have come after using elliptic curve cryptography to encrypt the data are:

Fig 5: Registration form for users into cloud

The client who wants to store their data safely into the cloud has to register in cloud databases as represents in fig 5.They have to register with their details(such as Email, Mobile number and designation).

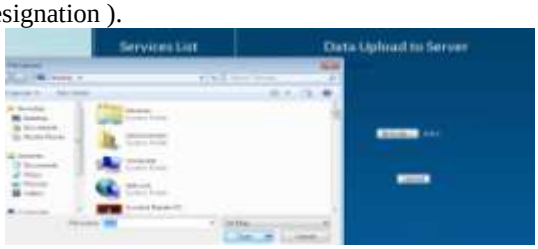

Fig 6: Storing a file into cloud

Once the user register into the cloud, they can store their data into the cloud safely for the future use. A file can be upload into the cloud storage as represented in fig 6.

Fig 7: Encrypting the data

The file which has been uploaded by the user is encoded and then stored in the cloud storage as represents in fig 6 .Encryption of data is done to keep the file in secure way so that only authorized party will handle by decrypting the file using their registration details.

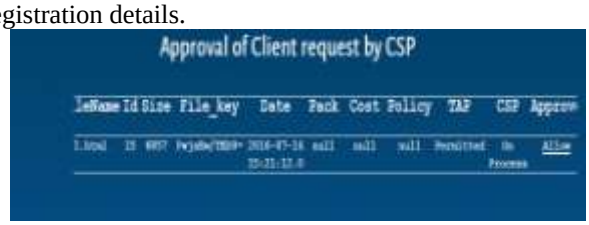

Fig 8: Approving client request by cloud service provider The administrator will check the authentication details of user and then approve the file to store into the cloud as represents in fig 8. This can help the user to store their data in a secure way.

Conclusion

Cloud computing safety design is important component in building up trust in Cloud Computing worldview. Trust in utilizing the cloud services relies upon trusted computing techniques, strong authorization and access control strategies, giving a safe execution environment, securing cloud interchanges, and supporting smaller scale structures. In this article it is examined about information security with the proposed technique to give secrecy and validation of information between clouds. The ECC can give same level and type of security as RSA based systems however with lesser key length comparatively. ECC based frameworks are along these lines in a perfect world suited for resource constraint equipment's which have computational, memory and power constraints. ECC based frameworks are along these lines getting to be critical for remote sensor systems, remote correspondence (wireless), smart card based applications and so on. ECC based frameworks are the Next Generation asymmetric cryptography frameworks.

REFERENCES (SIZE 10 & BOLD)

[1] Mr.Jayadip Sen "Security and privacy issues in Cloud Computing"
[2] Elsenpeter Robert, Anthony T.Velte and Toby J.Velthe "Cloud computing a practical approach"
[3] Farzadsabahi, "Cloud computing security threats and Responses", IEEE confer.2011,978-1-6128-486-2/111..
[4] LiuPeng, the definition and characteristics of cloud computing, http://blog.sina.com.cn/s/blog_5f0da5590100cmxw.html http://www.chinacloud.cn,
[5] Cloud Security "A Comprehensive Guide to secure Cloud Computing" Ronald L. Krutz and Russell DeanVines
[6] H. Takabi, S Kumaraswamy and S Latif "Cloud Security and Privacy", O'REILLY publication, first edition, Sept 2009.
[7] N. Gohring, "Amazon's S3 down for several hours,"- 2008 .
[8] G. Caronni and M. Waldvogel, "Establishing Trust in Distributed Storage Providers", In Third IEEE P2P conference, Linkoping 03, 2003
[9] F. Sebe. J. Domingo-Ferrer, and A.Martinez-Balleste. Y. Deswarte, and J.J. Quisquater,"Efficient Remote Data possession Checking in Critical Information Infrastructures" , IEEE Trans knowledge and Data Engineering vol.20, no.8,aug-2008

[10] P. Syam Kumar, R. Subramanian, "Homomorphic Distributed verification protocol for Ensuring Data Storage in Cloud Computing". Internation Journal of Information, VOL. 14, NO.10, OCT-2011,pp.3476.
[11] M A.Shah, M. Baker, J.C.Mogul, and R.Swaminathan,"Auditing to keep Online Storage Services Honest ",Proc.11th USENIX Workshop on in Operating systems,2007,pp.1-6,CA,USA.
[12] N. Oualha, M. Onen, Y. Roudier,.,"A Security Protocol For Self-Organizing Data Storage".Tech Rep.EURECOM+2399,InstituteEureco 2008, France.
[13] Ravi kantSahu and AbhishekMohta, L.K.Awasthi "Robust Data Integration while using Third Party Auditor for Cloud Data Storage Services",Conf. IJARCSSE,2012,volume2,Issue2,ISSN:2277128x.
[14] Qian Wang and Cong Wang and KuiRen,Wenjing Lou,Jinli "Enabling public Auditability and Data Dynamics for Storage Security in Cloud Computing " in IEEE transactions on parallel and distributed systems,2011,vol.22,no.5.
[15] Govinda V and Gurunathaprasad, H satshKumar."Third Party Auditing for Security data Storage in Cloud through digital signature using RSA",IJASATR,2012,issue 2,vol-4,Issn 2249-9954.
[16] M.Ashah and R.swaminathan and m.baker "Privacy-Preserving Audit and Extraction of Digital Contents",2011 .
[17] A.F. Barsoum and M.A. Hasan, "Provable possession and replication of data over cloud servers",Center for Applied Cryptographic Research(CACR),University of waterloo,Report2010/32,2010.
[18] L.Chen,G.Guo,"An efficient Remote Data Possession Checking in Cloud Storage", International Journal of Digital content Technology and its applications. Volume 5,Number 4,April 2011,pp.43-50
[19] C.Wang, Q.Wang, K.Ren,N. cao and W.Lou,"Towards Secure and Dependable Storage services in Cloud Computing",Accepted for publication in future issue. Computing.DOI:10.1109/TSC.2011.24 .
[20] Amazon.com, "Amazon Web Services (AWS)", Online at http://aws.amazon.com
[21] D. L. Ponemon, "Security of Cloud Computing Users," 2010.
[22] C. Almond, "A Practical Guide to Cloud Computing Security,"
[23] MeikoJensen ,JorgSehwenk et al., "On Technical Security, Issuesicloud Computing" IEEE.