International Journal of Engineering Research & Management Technology ISSN: 2348-4039

March- 2015 Volume 2, Issue-2

Email: editor@ijermt.org www.ijermt.org

# Providing Security by Implementing Elliptical Curve Cryptography

**DineshKumar**
StudentM.Tech (CSE)
SRM University
NCR Campus Modinagar

**RandeepKaur**
Student M.Tech (CSE)
GNDU University

**M.Mohan**
Assistant Professor
SRM University
NCR Campus Modinagar

**ABSTRACT** –
Cloud computing hottest research area due to its ability to reduce the costs associated with computing. Data applications are a great benefit to organizations, business, companies and many large scale and small scale industries. Cloud computing security is developing at very rapid pace which include computer security, network security, information security and data privacy. Cloud computing plays very vital role in protecting data, application and the related infrastructure with the help of policies, technologies, controls , and data tools. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments**.** Cloud computing's main benefits include resource consolidation, uniform management, and cost-effective operation; for the cloud user, benefits include on-demand capacity, low cost of ownership, and flexible pricing. However, the feature that brings such benefits, such as sharing and consolidation, also introduce security and privacy problems. Security and privacy issues resulting from the illegal and unethical use of information, and causing disclosure of confidential information, can significantly hinder user acceptance of cloud-based services.

**Keyword** – Cloud Computing, data security, RSA algorithm, Encryption, decryption

## 1. INTRODUCTION

In cloud computing, the word cloud means the internet and computing means the service. Hence cloud computing is the services which we deliver from the internet. Goal of cloud computing is to make use of increasing computing power to execute millions of instruction per second. Cloud computing is being used to minimize the usage cost of computing resourced. In cloud the only thing done at the user's end is to run the cloud interface software to connect the cloud. The front end includes user's computer and software required to access the cloud network. Back end includes various computers, servers and database systems that create the cloud. Real time examples are Gmail, Google, Google Calendar, and Amazon etc. [1]

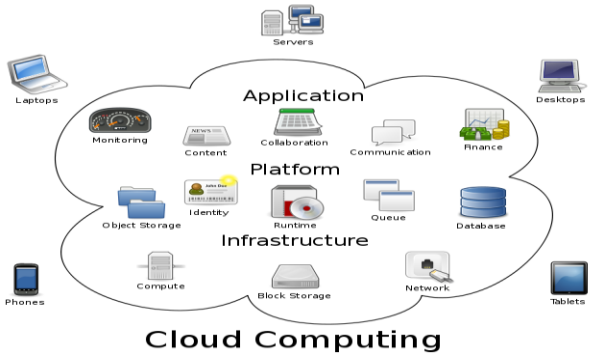


**Fig 1**

**1.1Characteristics: Cloud computing has a variety of characteristics:**

**On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

**Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

**Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

**Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

**Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

**1.2 Types of Cloud There are three types of cloud**

a) Public cloud
b) Private cloud
c) Hybrid cloud
d) Community cloud

**Public cloud:** It allows system and services to be easily accessible to general public eg. Google, Amazon, Microsoft offer services via internet.
Advantages: Cost effective, Reliable, Flexible, Location independent, Pay per use, highly scalable.
Disadvantages: Low security (resources are shared publically), Less customizable than private cloud.

**Private cloud:** It allows system and services to be easily accessible within an organization. Private cloud is operated within the single organization and managed internally.
Advantages: High privacy and security (resources are not shared publically and the location is limited), Cost and Energy efficient, More control.
Disadvantage: Restricted area, Inflexible pricing, Limited scalability.

**Hybrid cloud**: It is the type of cloud both the mixture of public and private cloud. Non critical activities are performed using public cloud while critical activities are performed using private cloud.
Advantages: Scalable, Flexible, Cost efficient, Secure.
Disadvantages: Infrastructure dependency, Security compliance.

**Community cloud:** It allows systems and services to be accessible by group of organizations. It share infrastructure between many organizations from specific communities.

Advantages: Cost effective, Sharing between many organizations, More secure.
Disadvantages: Authentication, It is also challenging to allocate responsibilities of governance, security and cost
Resources in cloud is seems that can be extended unlimitedly, got anytime, used on-demand and paid according to apply. It dynamically delivers everything as a service over the internet based on user demand, such as network, operating system, storage, hardware, software, and resources. These services are classified into three types:

Infrastructure as a Service (IaaS)
Platform as a Service (PaaS) and
Software as a Service (SaaS).[2]

**Infrastructure as a Service (IaaS):**
At the lowest level is **Infrastructure as a Service**. IaaS is as close to the "metal" as you can get. An IaaS service provider typically provides networked computers running in a hosted environment. At it simplest, the IaaS provides the hardware and, usually virtualized, OS.Every web hosting company out there could almost be considered an IaaS provider. The key differentiator between a web hosting provider and an IaaS provider is how they charge for their services. A web hosting company charges by the system by the month. An IaaS provider charges only for the compute power that is utilized (usually by CPU hours used by month).By this definition, some of the more well-known IaaS providers are:

- Amazon EC2 (elastic cloud compute)
- Rackspace
- Google Compute Engine

**Platform as a Service (PaaS):**
Somewhere in the middle is **Platform as a Service** (PaaS). The biggest difference between IaaS and PaaS is that PaaS adds support for the development environment (development language and application server technology).By writing your application in this environment you can very easily take advantage of dynamic scalability, automated database backups, and other platform services without the need to specifically code for it. For this reason, PaaS offerings generally support a specific set of programming languages or development environments.PaaS services are usually billed as an incremental cost on top of the IaaS monthly charges. For example, there may be a small monthly fee for the use of a load balancer or a database backup service.Some examples of the more popular PaaS providers are:

- Amazon AWS Elastic Beanstalk PaaS built on top of Amazons IaaS infrastructure. Supports Java (on Tomcat), PHP, Python, .Net and Node.js
- Google App Engine — Supports a subset of common Java environments as well as Python and Go.
- Cloud Foundry — Owned by VMWare. Supports Java, Ruby, Node.js and Scala.
- Engine Yard — Ruby on Rails, PHP and recently Node.js

**Software as a Service (SaaS):**
At the highest level is **Software as a Service**. SaaS delivers an application to a consumer or business user through a web browser client. The business logic and data for the application run on a server living somewhere on the network, not through an application running on the user's computer. The software is normally sold to the end user via a subscription, as opposed to a one time, upfront license fee.There are 1000s of examples of SaaS applications. One of the first, and still one of the best known, is Salesforce.com, which is an enterprise CRM tool. Other popular examples of SaaS applications are:

- Box.net
- Google Docs

- Microsoft Office 365
- Jira
- Basecamp

## 2. Cloud Security Issues

It is very important for the network that interconnect the systems in the cloud should be very secure. Resource allocation and memory management algorithm also have to be very secured.

Data Issue: As cloud is used as public network hence anyone from anywhere can access the data. This leads to the modification of data. Data stealing and data loss may also occur many times. [3]

It should be done at both side i.e. both at provider side and user side such that there is no threat of data stealing, data tampering etc.

## 3. Cloud Security

Data security and network security is the main hurdle in the cloud computing which lead to many security threats. Data within the cloud can be secured by many encryption techniques.

Encryption is the technique to convert our meaningful plain text to the cipher text so that no one can read and modify the data.

Decryption is the technique to convert the cipher text to the original plain text such that the authentic user can read the information.

Encryption/Decryption is basically the coding and decoding of the plain text which prevent the data threats such as data tampering, data modification, data stealing etc.. It provides the data confidentiality, data integrity, data authenticity etc..


### 3.1 Data Security in Cloud computing using Elliptical Curve Algorithm

ECC compare with RSA offer equal security for smaller key size by reducing processing overhead.

Brief review for abelian group

Abelian group G is denoted as {G, •} contsin set of elements where binary operation is denoted as • that associates to each ordered pair (a,b) of elements in G an element (a•b) in G such that G follows the following properties i.e.

Closure Property

Associative Property

Identity Property

Inverse Property

Commutative Property

Cubic equation for elliptical curve staken as follow

$y^2+axy+by=x^3+cx^2+dx+e$

where a,b,c,d,e are real number and x and y take on value in the real number. This equation is called Weierstrass equation.

**Elliptical curve over Zp**

$y^2 \text{mod} P = (x^3+ax+b) \text{mod } P$

P=(Xp,Yp)

Q=(Xq,Yq)

P is not equal to Q

R=P+Q=(Xr,Yr)

Where

$Xr=(\lambda^2-Xp-Xq) \text{mod} P$

$Yr=(\lambda(Xp-Xr)-Yp) \text{mod} P$

Where

$\lambda=[(Yq-Yp)/(Xq-Xp)] \text{mod} P$ if $P \neq Q$

$\lambda=[(3Xp^2-a)/2Yp] \text{mod} P$ if P=Q

Encryption and Decryption:

Encryption: Plain message m to be send as an Pm. It will point Pm that can be encrypted as cipher text and decrypted.

Pa = na*G(public key) where an is private key for A

Cm = Cipher text={kG,Pm+kPb} where k is any random positive integer choosen by A

G is any base point on define elliptical group of points Eq(a,b)

Pb is public key for B

Decryption: to decrypt B multiplies the first point in the pair by B's secret key and subtract the result from second point.

Pm+kPb-nb(kG) = Pm+(nbG)-nb(kG) = Pm

## 4. CONCLUSION

We can conclude that RSA algorithm secures our data but it has some drawbacks i.e. It is slower than secret key method but can be used in conjunction with secret key (symmetric) to make it more efficient. It can be vulnerable to impersonation if hacked.

RSA so far has not been broken but certain bad things can happen with it. Here are few things that can go wrong

a) Using small primes.

b) Using primes that are very close.

c) Two people using the same N, receiving the same value.

Factoring is thought to be hard.

To enhance the security more, a mechanism to secure the data integrity in security cloud can be area of research

**Advantages of ECC:**

- Smaller keys, ciphertexts and signatures.
- Very fast key generation.
- Moderately fast encryption and decryption.
- Special curves with bilinear pairings allow new-fangled crypto.
- Binary curves are really fast in hardware.[5]

## 5. REFERENCES

1. Venkata narasimha inukollu, Sailaja Arsi, Srinivasa Rao Ravuri . "Security Issues Associated with Big Data in Cloud Computing". International Journal of Network Security & its Application (IJNSA), Vol. 6, No. 3, May 2014
2. Neha Jain , Gurpreet Kaur. " Implementing DES Algorithm in Cloud for Data Security". VSRD International Journal of CS & IT Vol. 2 (4), 2012
3. Dr. A.Padmapriya, P.Subhasri . "Cloud Computing: Security Challenges & Encryption Practices". International Journal of Advanced Research in Computer Science and Software Engg 3 (4),March - 2013, pp. 255-259
4. N.Padmaja, Priyanka Koduru. "Providing Data Security in Cloud Computing using public key cryptography". International Journal of Engineering Sciences Research-IJESR Vol 04, Special Issue 01, 2013
5. www.quora.com
6. Dinesh Kumar,Randeep Kaur, Anant Gaur, M.Mohan "Security of data with in cloud". International Journal of Engineering Research & Management Technology, Page 26, January- 2015 Volume 2, Issue-1