**1. INTRODUCTION**

**1.1 PURPOSE**

Cloud Computing is the style of computing where the resources are provided as services on internet. There are three types of services in Cloud Computing which are used for the deployment of the application on the cloud. Data on the cloud will become more scalable, Reliable and Secure. The big players in Cloud Computing are Amazon, Google, Microsoft and IBM. Cloud Computing is based on five attributes such as Shared Resources, Scalability, Pay as U use, Elasticity and Self Provisioning of Resource. Most of the enterprises shifting their applications on to the cloud owing to its speed of implementation and deployment, improved customer experience, scalability, and cost control. The services in Cloud Computing are **SaaS**, **PaaS, laaS** amongst which we are using PaaS and laaS service for deployment of Application on the Cloud in our Project. This service exhibits five essential characteristics such As Rapid Elasticity, Resource Pooling, on demand Self-service, Broad Network Areas. Data is being transmitted between two clouds so in order to secure the data most of the systems use the combination of techniques, including:

• Encryption- It is used to encode the data in such a way that third party will not be able to hack that data.

• Authentication- It is used to create a separate user ID and Password so that only the authorized users will able to access the data.

•Separation of duties- In which accessibility is provided to all the users according to their priority.

These security parameters are achieved due to which the performance will gets increased and therefore the Security is obtained up to higher extent. Data security and privacy risks have become the primary concern for people to shift to cloud computing. Cloud Computing is mainly used for the improving the data handling capability where the services and the resources will be delivered continuously when and where required due to which the Cloud computing is in great demand. However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing Cloud is the free space where the application is being saved securely and the services are being provided continuously when and where required.

1

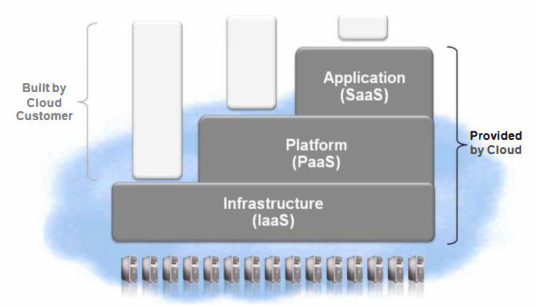
**Cloud Deployment Models**:

A*. Public Cloud*: The Cloud infrastructure is made available for the large industry group and general public provided by single service provider.

B. *Private Cloud*: The Organization can store the data on private Cloud. The main Advantage of this Cloud is Security of Data and Quality of Service.

C. *Community Cloud*: The Cloud Infrastructure is shared by many Organizations.

D. *Hybrid Cloud*: Two or more Clouds combine to form Hybrid Cloud.



**Cloud Characteristics:**

A*. Easy Use*- Most Cloud Provider will offer the Internet interfaces which are much simple so user can easily access the cloud services.

B. *Ubiquitous Network Access*- Cloud provides services through the standard terminal such as phones, Laptops, Mobiles.

C. *On demand Services*- Cloud is a pool of resources and services so we can get the services and resources by paying particular amount as required.

D. *Business Model*-Cloud is a Business Model because it is pay per use of service or resource.

E. *Pay as U Used* - Users have to pay for only the Resources they are using. Whenever the users need some resources then they have to pay for the particular resource as and when required.

2

**1.2 OBJECTIVE**

The primary goal of this project is to provide and simulate an effective solution to face the challenges and solve security issues that exists in cloud computing. Cloud Computing is the impending need of computing which is used for the IT Industries It is one of the hottest topic in research areas. Scalability and Flexibility increases for the computing services. Cloud Computing is the fastest growing technology for IT Industry. The Information is being transmitted via the network therefore security is one of the main problems or issue. The Application is deployed on the Cloud and for the secure transmission of the data we will be using ECC Algorithm in our project because of its advantages in terms of CPU utilization, time for Encryption and Key Size. This Project will explore the deployment of Application on the Cloud and increases the security level by implementing ECC & ECDH Algorithm, and AES Algorithm for secure file handling and Encryption.

**1.3 MOTIVATION**

Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms are developed in order to improve the security of data, but they having their own issues. Now in these days the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography use for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC propose equivalent security with smaller key sizes; these results in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is peculiarly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity.

Therefore, a new encryption standard is required that can fulfil the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithm using ECC, ECDH and AES algorithms along with encryption techniques.

3

**1.4 DEFINITION AND OVERVIEW**

Cloud Computing is the primitive change happening in the field of Information Technology. It uses the internet technologies for delivery of IT - enabled capabilities 'as a service' to any needed users. Cloud computing enables users to access resources using internet, from anywhere at any time without worrying about technical/physical management and maintenance concern of the original resources. In its description for cloud characteristics The US National Institute of Standards and Technology (NIST) defines as cloud characteristics the following: On-demand self-service, Ubiquitous network access, Resource pooling, Rapid elasticity (resources can be scaled up and down easily), Metered service (resources' usage is measured) and Pay-As-You-Consume business models. Google Apps is an important example of Cloud computing; it enables to access services through the browser and brought into effective action on millions of machines over the Internet. One of the most prominent service offered by cloud computing is cloud storage. Cloud storage is simply a term that refers to on line space that you can use to store your data. In more strict way, cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network.

**Software as a service (SaaS)**

The cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The cloud consumers have limited administrative control of the applications.

**Platform as a service (PaaS)**

The Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components. The PaaS Cloud Provider typically also supports the development, deployment and management process of the PaaS Cloud Consumer by providing tools such as integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), deployment and management tools.

**Infrastructure as a service (IaaS)**

The Cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure. The Cloud Provider runs the cloud software necessary to makes computing resources available to the IaaS Cloud Consumer through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces.

4

The whole idea and definition of this project lies in its name i.e. **Secure Cloud**, which aims at providing and simulating an effective solution to face the challenges and solve security issues that exists in cloud computing. But first we should look at some of the frequently occurring issues in cloud computing mostly during the transmission of data. Some of them are discussed below:

A. *Encryption*- The message send by the sender i.e. the original message is being encrypted in such a way that third party will not be able to hack or misuse the data.

B. *Intrusion Detection and Prevention*- Data that is being entered and going out of the Network has to know.

C. *Separation of Duties*- Due to the insufficient communication between the expertise System misconfiguration takes place.

D. *Location of Data*- Every Organization will have different requirements and their access control on their data to be placed. A level of security is required to fulfil the customer need.

Sharing of Cloud Infrastructure could lead to the privacy issues. The Location of data could influence the privacy obligations. For storage and processing of data. Data leakage could also occur due to failure of security access rights. In order to secure the data stored on the cloud various security Algorithms are present which will help to encrypt the data before transmission in order to protect the valuable data from the hackers.

One of the better solution for maintain the security is cryptography which is basically used for protecting the data. **Public Key Cryptography**- In this cryptography different keys are used for Encryption and Decryption. **Secret Key Cryptography**- A key which is used for Encryption as well as Decryption is called Secret Key Cryptography. There are many Security Algorithms Each Algorithm have their own properties such as Key Size, Throughput, Performance, Encryption Decryption Time etc. By Comparing the Encryption Algorithms, we found out that ECC Algorithm is one of the best Algorithm which is having the high level of Security and better performance.

* **Elliptic Curve Cryptography(ECC)**:

Elliptic curve systems were first proposed in 1985 by Neal Koblitz and Victor Miller. An Elliptic curve over a field K have a set of points(Xi,Yi) in a plane. The set is finite and is denoted by E. It is one of the most secure Algorithm. ECC is a public key

5

cryptography Algorithm in which each and every user has its own pair of private and public key. Group Operator is an important one in ECC and is denoted by the symbol '+'. The Standard form of ECC is given by y2 =x3 + ax + b for some fixed values for parameters a and b. The security of ECC Algorithm depends on the ability of computation of new points on the curve and then the encryption of these points as information is to be exchanged between the end users. Group Operator is used to find P which is one of the point on the curve. Again, this operator proceeds the computation as P+P, P+P+P, ..............

Which makes it very difficult for the hacker to hack the data.

* **Key Agreement using ECDH Algorithm**:

Both clouds i.e. Cloud A and Cloud B will agree for the data which is being transmitted The Agreement between the two parties will takes place only when both the keys are same.

I)A will select an integer XA = klas his/her private key. The public key for A will be Y A = XA x P, which implies that when the private key is an ordinary integer, the public key is a point like P.

2) B does exactly the same thing it selects an integer XB = K2 as his/her private key, with the public key for B being YB =XB xP. Then both the parties exchange their public keys.

3) A computes the session key by KA = XAxYB = klxk2xP

4) B computes the session key by KB = XBxY A = K2xkl xP. Obviously, KA = K

This proves the Agreement for exchanging the Data between two parties and the generation of public and private key.

* **Key Generation:**

Algorithm generates both the public key and private key. Here Sender will be used to encrypt the data and receiver i.e. B is used to decrypt the data by using its own private key.

* **Encryption:**

Let m be the message that has been sent from the sender A to B. Sender A will encode the message and on the way of transmission only the encryption will take place and for the transmission of data only few nano seconds will be required to travel the data to receiver.

6