

Two way authentication over cloud using elliptic curve cryptography

A Dissertation

Submitted

By

Navalpreet Kaur

(Regd. No. 11311334)

To

Department of Computer Science and Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in

(Computer Science and Engineering)

Under the guidance of

Mr. Harsimran Singh

(Asst. Prof., UID- 18273)

(May 2015)

ABSTRACT

Today, a huge number of organizations are moving towards cloud for storing a huge amount of data. Security is the most significant concern in cloud. There are several security problems of cloud computing which are related to trust, data confidentiality, authentication, access control etc. These problems crack the CIA triad of cloud. The influence of data security and the range of loss that is suffered due to unauthorized access to cloud data motivates to take the problem as a challenge and come up with feasible solutions that can protect the data from theft, mishandling. Many authentication techniques are available in cloud computing but some are efficient in terms of time and some are attack resistant. But the need is to propose a technique that is the combination of both. The algorithms named Modified Diffie Hellmann and Elliptic Curve Cryptography solves the problem of security of data in cloud.

ACKNOWLEDGEMENT

I would like to take this opportunity to express my deep sense of gratitude to all who helped me directly or indirectly during thesis work.

Firstly, I would like to thank my supervisor Mr. Harsimran Singh for being great mentor and best adviser I could ever have. His advice, encouragement and critics are sources of innovative ideas, inspiration and cause behind the successful completion of this dissertation. I am highly obliged to all faculty members of computer science and engineering department for their support and encouragement.

I would like to express my sincere appreciation and gratitude towards my friends for their encouragement, consistent support and invaluable suggestions at the time I needed the most.

I am grateful to my family for their love, support and prayers.

Navalpreet Kaur

Regd no. 11311334

DECLARATION

I, NAVALPREET KAUR hereby declare that the dissertation proposal entitled '**Two way authentication over Cloud using elliptic curve cryptography**', submitted for the M.Tech (Computer Science and Engineering) degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:
Kaur

Investigator: Navalpreet

Regd. No.: 11311334

CERTIFICATION

This is to certify that **NAVALPREET KAUR** has completed M. Tech dissertation titled **‘Two way authentication over Cloud using Elliptic Curve Cryptography’** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation is fit for the submission and the partial fulfillment of the conditions of the condition for the award of M.Tech Computer Science and Engineering.

Date:

Signature of Guide

Name: Mr. Harsimran Singh

UID: 18273

Contents

1.2 Cloud Computing Evolution	2
1.3 Characteristics of Cloud Computing.....	5
1.4 Cloud Computing Services	6
1.5 Deployment Models of Cloud Computing	7
1.6 Major Concerns of Cloud Computing.....	9
1.7 Disadvantages of cloud computing.....	9
Cloud computing has many advantages as well as the disadvantages as.....	9
• Security and privacy in the Cloud	9
1.8 Cloud Resource Management.....	10
1.9 Security in Cloud	12
CHAPTER 2	13
LITERATURE REVIEW	13
CHAPTER 3	22
3.1 Problem Formulation	22
3.2 Objectives of Research.....	23
3.3 Research Methodology	23
3.5 Tools.....	27
CHAPTER 4	29
RESULTS AND DISCUSSIONS.....	29
4.1 Implementation of the Proposed Technique.....	29
CHAPTER 5	42
Conclusion and Future Scope.....	42
4.1 Conclusion and future scope:	42

CHAPTER 1

INTRODUCTION

This chapter introduces Cloud computing, its evolution, Cloud characteristics and the services offered by Cloud.

1.1 Introduction

Cloud Computing,” to place it basically, means “Online Network Computing.” The Online Network is normally envisioned as clouds; the term “cloud computing” for calculation done through the Online Network. With Cloud Computing, clients can use data storage resources through the online network from anyplace, for as long as they need, without worrying about any maintenance of actual resources. Also, data storage in cloud is very active and accessible. Cloud computing is dissimilar to grid computing, utility computing, or autonomic computing. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be organized on thousands of computer through the Internet.

1.2 Cloud Computing Evolution

In Fig 1.1, explaining the evolution of cloud computing where we have three phases that is mainframe computing, distributed computing and cloud computing.

EVOLUTION of COMPUTING

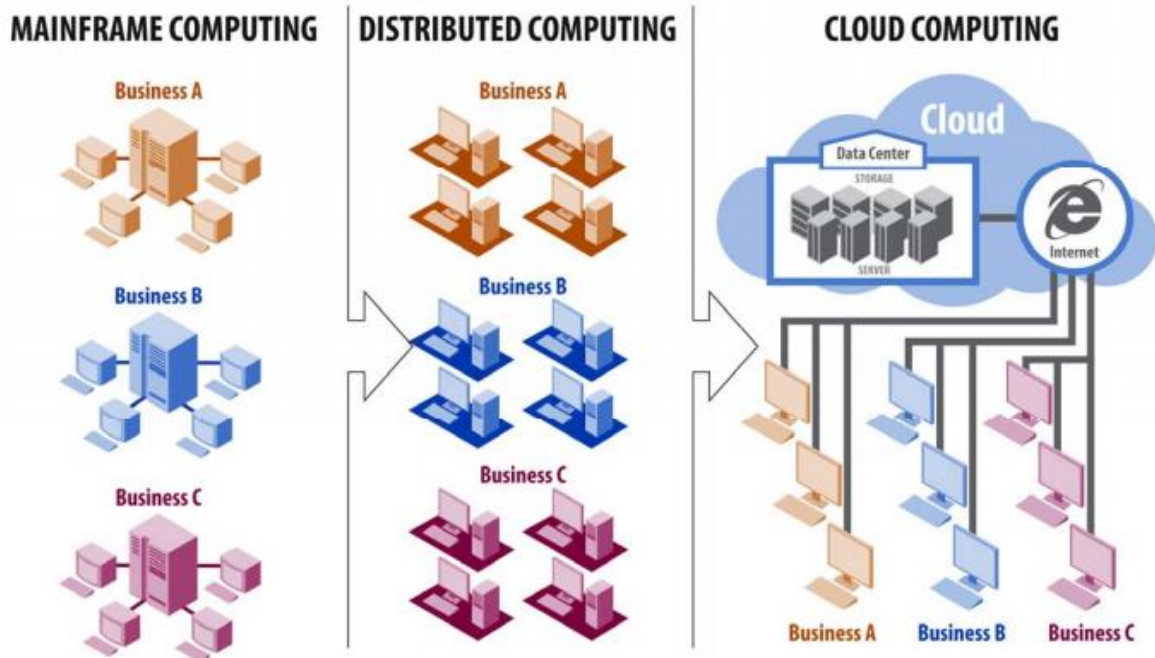


Fig 1.1 Evolution of Cloud Computing[1]

Phase I: Mainframe Computing

In the past, companies powered their information infrastructure from a mainframe. In one physical location (i.e. a building or an office), this large, powerful computer stored data and ran all the software applications. While it was relatively easy to support multiple applications through one mainframe, maintaining such a large piece of hardware was expensive and inefficient. [1]

Phase II: Distributed Computing

As lower cost computing became more available (enter the IBM PC in 1981) and as more people wanted access to more powerful applications, mainframe computing became less effective. The next solution for businesses was to replace the mainframe with multiple cheaper computers, each with enough computing power to store data and run applications. In a sense, this computing solution was easier to manage; whereas one bug within the mainframe could shut down every computer relying on it, each cheaper computer ran independently. However, this independence meant that the computers didn't coordinate with

each other; data sharing was difficult and any resources saved were negated because each computer had to be changed/fixed/updated individually. [1]

Phase III: Cloud Computing

Luckily for us, today we have the cloud, which offers a slew of advantages to the computing world. As a very general definition, the cloud is a shared network of computers through which people and companies store data and run software. At its core, the cloud is a data center, a physical building with hardware (computers) and software running on that hardware, connected by pipes and routing to many, many computers. Cloud providers, who manage and maintain these networks, offer “services” rather than “products” in that clients are allowed to access and use the cloud, but they do not “own” any part of it; there is no hardware or software installation. [1]

The Best of Both Worlds

At the most basic level, two factors go into the total cost of ownership of a computing solution: cost and ongoing support. Mainframe computing offered centralized management, as all the data and applications were centered in the mainframe. However, mainframes and their maintenance were extremely expensive; only large, well-established companies could afford mainframe computing. With distributed computing, companies could buy cheaper, individual computers rather than paying for an expensive mainframe. This made computing more scalable and thus more accessible to smaller companies. However, distributed computing still wasn't an ideal computing solution because without a way to centrally manage all the computers, it was too difficult to support. Cloud computing offers the central management and coordination of mainframe computing with the affordability and scalability of distributed computing. It is therefore an ideal solution for both large and small companies.[1]

NIST (National Institute of Standards and Technology) defines the cloud computing as follows:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[2]

1.3 Characteristics of Cloud Computing

The National Institute of Standards and Technology (NIST) has published an official definition of the cloud, which includes five essential characteristics of every cloud. [3]

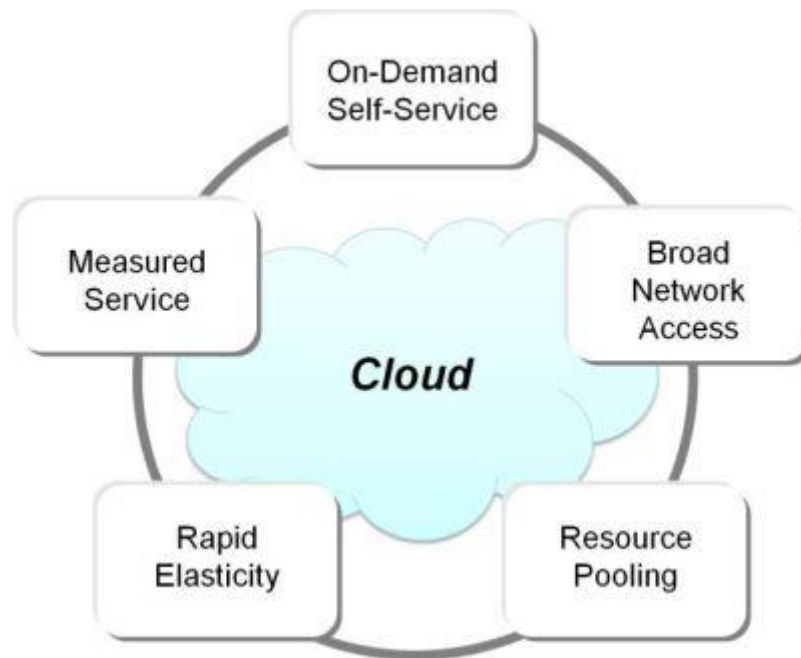


Fig 1.2 Characteristics of Cloud Computing [4]

- **On-demand self-service.** In on-demand self-service, client can determine how much capability like network storage and server time is needed from the cloud without interaction with service's provider.
- **Broad network access.** Services is provided over the web and can be accessed that services through standard type of clients like mobile phones, laptops and tablets.
- **Resource pooling.** The cloud is capable to serve several clients by sharing its computing resources and allocate/reallocate them according to demand. The clients have no knowledge about the exact location where the data is placed. Examples of resources like memory, virtual machines, storage, bandwidth etc.

- **Rapid elasticity.** The clients have capabilities to decrease or increase the cloud services easily.
- **Measured service.** The cloud can automatically control the resources used by a client that is measurable and charged by cloud provider.

1.4 Cloud Computing Services

Cloud providers offer multiple levels of services, depending on the client's needs.[3] as shown in figure 1.3

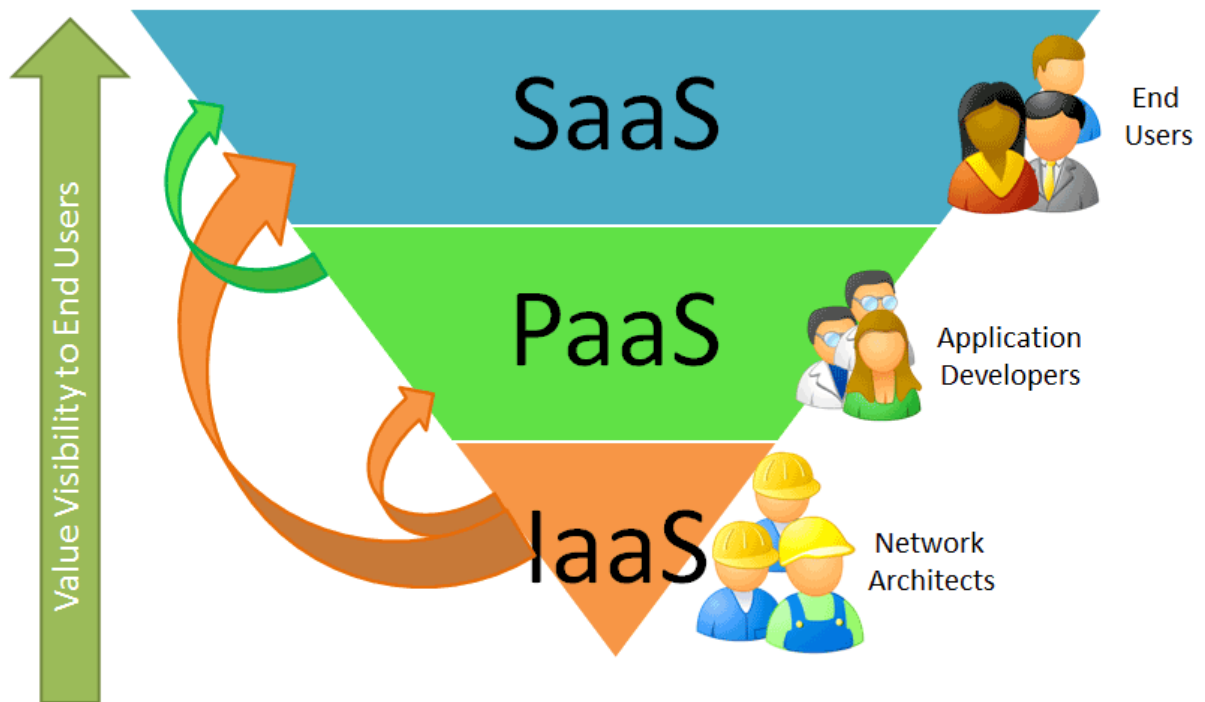


Fig 1.3 Services of Cloud Computing [4]

- **Infrastructure as a Service(IaaS)**

Infrastructure as a Service is the basic level of cloud service. It is the delivery of hardware and associated software as a service. Customers using IaaS mostly buy an operating system and cloud provider manages the memory, processing and system's CPU. Examples of IaaS are Amazon Web Services Elastic Compute(EC2) and Secure Storage Service (S3), 3 Tera, GoGrid etc.

- **Platform as a Service (PaaS)**

Platform as a service (PaaS) is the next level of cloud service. Service provider of cloud provides development and deployment platform delivered as a service over the internet. This platform consists of infrastructure software and includes database , middleware and development tools. Examples of PaaS is Google Apps Engine , LAMP platform(Linux, Apache, MySql and PHP).

- **Software as a Service (SaaS)**

Software as a service (SaaS) is the three level of services in cloud. In this service, all the application is offered to the customer, as a service on demand. Data of this service is stored in the Cloud , so that customer can interact with the application through web browser. A single service runs on the cloud and several users are accessed. Examples of SaaS is Google, Salesforce and Microsoft etc.

1.5 Deployment Models of Cloud Computing

There are four deployment options for the cloud: private cloud, community cloud, public cloud and hybrid cloud.[3] as shown in figure 1.4

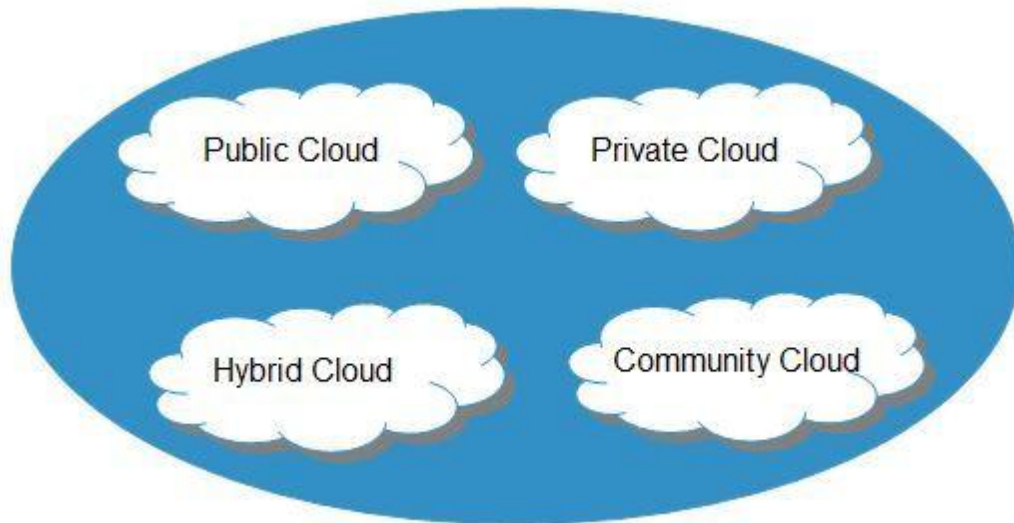


Fig 1.4 Deployment models of Cloud Computing

- Public Cloud

Public Cloud is the common deployment model of cloud computing where services are available to anyone on web as pay-as-you-go. In public cloud, there are many datacenters built by public Cloud providers. Examples of Public Cloud are Amazon Web Services (AWS), Google App Engine. Amazon EC2 provides IaaS , Google App Engine provides PaaS and Salesforce.com provides SaaS.

- Private Cloud

Private Cloud is deployed within organization to provide services for internal users. Private Cloud services provide control over the infrastructure and improving security because its access is restricted to one organization.

- Community Cloud

Community Cloud is deployed to specific community of consumers from organizations.

- Hybrid Cloud

Hybrid Cloud is deployed two or more cloud infrastructures (public, private, or community). With a Hybrid Cloud, service providers can utilize third party cloud providers that increasing the flexibility of computing.

1.6 Major Concerns of Cloud Computing

The major concerns about cloud computing are **security** and **privacy**. The idea of handing important data another company worries about some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key. Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy. One way is to use **authentication** techniques such as user names and passwords. Another is to employ an **authorization** format; each user can access only the data and applications relevant to his or her job.

1.7 Disadvantages of cloud computing

Cloud computing has many advantages as well as the disadvantages as,

- **Security and privacy in the Cloud:** Security is the biggest concern when it comes to cloud computing. In a cloud based infrastructure, a company gives the private data and information. This information may be sensitive or confidential. The cloud service provider helps to manage, protect and retain the information. Hence the provider's reliability is very critical. Similarly, privacy in the cloud is another huge issue. Companies and users have to trust their cloud service vendors that they will protect their data from unauthorized users. The various stories of data loss and password leakage in the media does not help to reassure some of the most concerned users.

- **Dependency and vendor lock-in:** One of the major disadvantages of cloud computing is the implicit dependency on the provider. The implicit dependency is known as vendor lock in. If a user wants to switch from one service provider to another then it can be very painful and cumbersome to transfer huge data from the old provider to the new one
- **Technical Difficulties and Downtime:** Certainly the smaller business will enjoy not having to deal with the daily technical issues and will prefer handing those to an established IT company. Hence in the cloud computing you should keep in mind that all systems might face dysfunctions from time to time. Outage and downtime is possible even to the best cloud service providers.
- **Limited control and flexibility:** In the cloud computing, the applications and services run on remote, third party virtual environments, companies. The users have limited control over the function and execution of the hardware and software. Hence, remote software is being used, it usually lacks the features of an application running locally.
- **Increased Vulnerability:** The cloud based solutions are exposed on the public internet and are thus a more vulnerable target for malicious users and hackers. On the internet nothing is completely secure. Hence people may suffer from serious attacks and security breaches. It happens due to the interdependency of the system

1.8 Cloud Resource Management

A cloud computing infrastructure is a complex system containing a large number of shared resources. Cloud resources are same as the resources present in the surroundings except that cloud resources are placed remotely. There are three aspects of cloud resource management:

- Performance management
- IT Security
- Provisioning

1.8.1 Performance management

Cloud performance management is the management of software services running in the cloud and computing systems. The impact of performance can be countered when services are connected between cloud and user's computing services. When a user moves his applications to the cloud, he must change his application configuration and network topologies.

1.8.2 IT Security

IT security is the most important concern of cloud computing. The cloud service provider provides good deal of IT security. Customers want IT security to integrate with their own data centers.

Cloud Service Provider implements IT security

- Protection of customers from external threats.
- Isolation of customer environment from one another.

As a customer take into following consideration

- Full understanding of hardware and software i.e. firewalls, detection system, Virtual Private Networks.
- Knows how the cloud providers are providing security to your overall system.

1.8.3 Provisioning

It is the responsibility of cloud service provider to maintain and provision cloud resources. The customer expects provisioning of resources is to be automate and immediate in case of SaaS. But in case of Pass and IaaS, no doubt the situation is same but user may need to request additional resources because in both the cases users can directly manage the cloud resources.

1.9 Security in Cloud

Security is the one of the most challenging issues in IT world. A large amount of data is stored at cloud. To protect the confidential data from unauthorized access, there is a great need of security in cloud computing environments. Many levels of security are required in cloud environment.

Access Control: There should be right level of access control for the resources in the cloud environment to protect the cloud for security purpose.

Authentication and Authorization: It refers to testing user's identity and give him privileges to access the resources and authorized data. There must be procedures and methodologies just like digital signature and encryption used in network security so that only right people can change the data or application.

Identity and access management: The features of IAM are authentication, authorization and auditing of the users accessing cloud resources. There is trust boundary between organization which can be controlled and monitored for the applications deployed on the cloud.

LITERATURE REVIEW

During past few years, cloud computing has been growing very fast. It is one of the today's most inspiring technologies. It has grown from being an encouraging business knowledge to one of the fastest growing part of the IT industry. It is most exciting because of it does reduce cost associated with it while growing flexibility and scalability for processes and resources. Due to increasing demand for cloud, security is the main concern for IT world. The literature survey presents the stature of cloud security world and the various techniques available for protecting data from unauthorized access, most of the papers studied during the course brought refining of thoughts for various techniques.

1. FarazFatemi etal.(2014)

[6] Cloud Computing is an emerging technology having a lot of problems related to security, user authentication and access control. Ensuring security in cloud environments is the most challenging issue. Controlling the simultaneous accesses and operations in shared files is the other challenge during user authentication when the number of end-users is increased. This paper provides an efficient and scalable user authentication scheme for cloud environments by using various tools and techniques and the concept of agents like Client User Authentication (CUA) and Modified Diffie Hellmann Agent(MDHA). Two separate servers are used for storing authentication and cryptographic resources to decrease the dependency of user authentication and encryption process from main servers. Evaluation of the proposed model has been done according to various parameters- Scalability, Efficiency, and Security.

2. Ms Bhavana Sharma.(2013)

Cloud computing is a model for allowing suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction.[7] Elliptic Curve Cryptography

Algorithm offers secure message integrity and message authentication, along with non-repudiation of message and data confidentiality. Cryptography is the future technologies in the field of data security over to the web. Cloud Computing is the computing as a utility that shifts customer programs and data from personal computers to the clouds, providing all kinds of resources over the Internet. This paper introduces the existing issues in cloud computing along with network security.[7]

3. Veerraju Gampala et al. (2012)

Cloud computing is one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing is Internet based computing due to shared resources, software and information are provided to consumers on demand dynamically. Cloud computing is one of the fastest growing technology of the IT trade for business. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper will explore data security of cloud in cloud computing by implementing digital signature and encryption with elliptic curve cryptography.[8]

Now a day's cloud computing facing many security challenges. Users put their data in the cloud and transfer from one cloud to another, the privacy of users at risk result from last control of data. Users most concerned about data security, so virtualization security and data security are the main problem of the cloud computing security. We concern here data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds. In future we will concern more security issues of cloud computing and try to find better solutions using cryptography.

4. Deyan Chen et al.(2012)

It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud.[9]

According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues exist in all levels in SPI service delivery models and in all stages of data life cycle. The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. According to the analysis for data security and privacy protection issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defense in depth. Regarding privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of cloud-based applications.

5. Pragnesh G. Patel et al.(2013)

Computing is one of the rapidly growing field of IT which is used to unite power of various resources in a more efficient and scalable way to the end user. In cloud computing, all the data of users are transferred over the network or stored in the cloud. So there is a great risk of security vulnerabilities on the user's data. This paper presents an elliptic curve cryptography based encryption and decryption algorithm to provide security of data while at data center or at the network. The algorithm was implemented by creating a cloud environment using openstack. The comparison of this algorithm was made with other conventional algorithms like DES, 3DES and RSA by simulation using cloudSim simulator. The results showed that throughput of ECC based algorithm is high as compared to other algorithm because of small key size of ECC as compared to others.[10]

6. MahmoodKhalelIbrahem proposes a zero knowledge proof protocol by modifying diffie hellmann key exchange algorithm. Two versions of the proposed protocol are presented which solves the problem of man in the middle attack in D-H key exchange algorithm. The version 1 is still vulnerable against man in the middle attack. To protect the proposed algorithm from this attack, version 2 provides mutual authentication to prove that the server is honest. Analysis of the protocol shows that it satisfies the ZKP properties and resist against various attacks like discrete logarithmic attacks and main in the middle attacks. The proposed algorithm serves as the key exchange algorithm along with providing authentication services.

7. NehaTirthani et al. Technological advancements in cloud computing due to increased connectivity has resulted in migration towards cloud computing. With a promising technology, it sometimes hinder user's privacy, putting new security threats in data on cloud The paper discusses the basics of cloud computing along with its security issues. The time consuming encryption calculations and voluminous data have been proved as a hindrance in this field. To overcome this problem, the non breakability of Elliptic curve cryptography for data encryption and Diffie Hellmann Key Exchange mechanism for connection establishment have been used. The main advantage of this scheme is that the cryptosystems that rely on Elliptic Curve Discrete Logarithmic Problem (ECDLP) provides high strength per bit because there is no subexponential time algorithm to solve ECDLP in selected elliptic curve group. ECC is very attractive in areas where memory limitations and computational overhead is a concern.

8. Uma Somani et al. Cloud computing is the internet based technology that provides dynamic resource pools, virtualization and high availability. The prevalent problem associated with cloud computing is the cloud security and appropriate implementation of cloud over the network. This paper uses the concept of digital signatures along with RSA algorithm, to encrypt the data while transferring over the network. This technique solves the dual problem of authentication and security. The approach uses digital signatures along with the Diffie Hellmann in order to authenticate client and server. After the authentication process, the user data is split and encrypted using RSA algorithm and sent to server for further computation. This paper compares RSA and AES algorithm in terms of key size and concluded that asymmetric encryption algorithm provides high security with the increased key size.

8. **C. Tien-Ho Chen et al.** propose an ECC dynamic ID based remote mutual authentication scheme for remote devices. It overcomes the flaws of Yang and Change's scheme that was proposed in 2009. The protocol consists of three phases- initialization, user registration and mutual authentication with key agreement phase. The proposed scheme is highly secured mutual authentication. It not only inherits the merits of ECC-based mechanism but also provides ID-based authentication with higher security for cloud computing.

10. M.Prabu et al proposes an approach to solve the real time implementation based on the finite fields. The elliptic curve cryptography is defined over two finite fields named prime field $F(p)$ and Binary field $F(2^m)$. The equation of elliptic curve over a prime field is:

$$y^2 \text{ mod } p = x^3 + ax + b \text{ mod } p$$

where $4a^3 + 27b^2 \text{ mod } p \neq 0$, a and b are real numbers, x and y take on values in the real numbers.

The equation of elliptic curve over a finite field is:

$$y^2 + xy = x^3 + ax^2 + b$$

This paper provides the basics of elliptic curve cryptography along with its advantages and applications. The inverse operation of ECC gets harder against increasing key length than the inverse operations in Diffie Hellmann and RSA. So, ECC implementations are more efficient than other implementations. Also the comparison of ECC was done with other cryptographic algorithms on the basis of key size which shows that ECC offers same level of security with small key size as provided by RSA and it is the best known algorithm for solving elliptic curve discrete logarithmic problems.

11. ParsiKalpana et al. discusses the security and privacy issues in cloud computing and proposes an RSA algorithm to encrypt the data before storing in cloud servers. RSA algorithm involves three steps: key generation, encryption and decryption. Key generation takes place between cloud service provider and the user. The proposed work allows only authorized users to access the data stored in cloud. If an intruder gets data accidentally he cannot decrypt it and get the original plaintext.

3.1 Problem Formulation

The main problem cloud computing faces today is to preserve confidentiality and integrity of data. Organizations use cloud in a variety of different service models and deployment models. A large number of security issues are associated with cloud computing, these are issues faced by cloud service provider and security issues faced by their customers. Some of these issues are:

1) Privacy: Security of the personal information of customer is very important in cloud computing. Public cloud is the one of the dominant architecture where cost reduction is concerned but relying on a cloud service provider to hold customer information raises many security concerns.

2) Trust: One of the main issue that cloud computing faces today is the trust between CSP and customers. Lack of customer trust causes many problems during deployment of cloud services. SLA is the only legal document which is the solution to resolve this problem which contains information of what providers is doing and willing to do.

3) Multi-tenancy: Storage, services, network and computational resources are shared among cloud systems to achieve better utilization and decreased cost that is called multi-tenancy. The confidentiality of data is hampered by sharing of resources. Virtual machines attacks and shared resources are the issues of multi-tenancy.

4) Key Management: Key management issue is the major issue in cloud computing. In the traditional encryption techniques single key is used for both encryption and decryption. But this might not be possible in case of complex problems. Customer must control and manage their key management systems because encryption keys cannot be stored on cloud.

Researchers developed a new method called two-level encryption which allows key management system to be stored on cloud that is somewhat efficient method.

5) Lack of User Control: It is the responsibility of service provider to control data stored in cloud. The whole sensitive information is located at the remote server therefore has a danger of theft, misuse etc. Also it is very difficult to get deleted data back from the cloud.

3.2 Objectives of Research

Objective of thesis divides the thesis into different levels which will be achieved one after the other. It defines the task to be performed during whole thesis.

In reference to the objective of the thesis, we will first study the various techniques and methods of authentication and will come to the conclusion that which one is the better in cloud environment. Then we will analyze the steps of best authentication scheme and then focuses on the drawbacks of the same scheme.

Later we will propose an efficient way of user authentication technique which will be better suited over the cloud environment. Here our main objective is to come out with a scheme of authentication which makes security over the cloud tighter. Along with that we will also try to focus on the security of the user's data which will be stored on cloud in the encrypted form. After that the whole proposed scheme will be implemented on the cloudsim using java language for the performance evaluation. Since JAVA supports the distributed programming, it will be much easier to use such language for implementation of cloud environment along with the proposed scheme. The overall steps during whole thesis are briefly summarized below:

1. To study various authentication schemes in cloud environments.
2. To propose an efficient user authentication technique.
3. Implement the scheme in cloud environment by using CloudSim simulator.
4. Performance evaluation of the proposed scheme.

3.3 Research Methodology

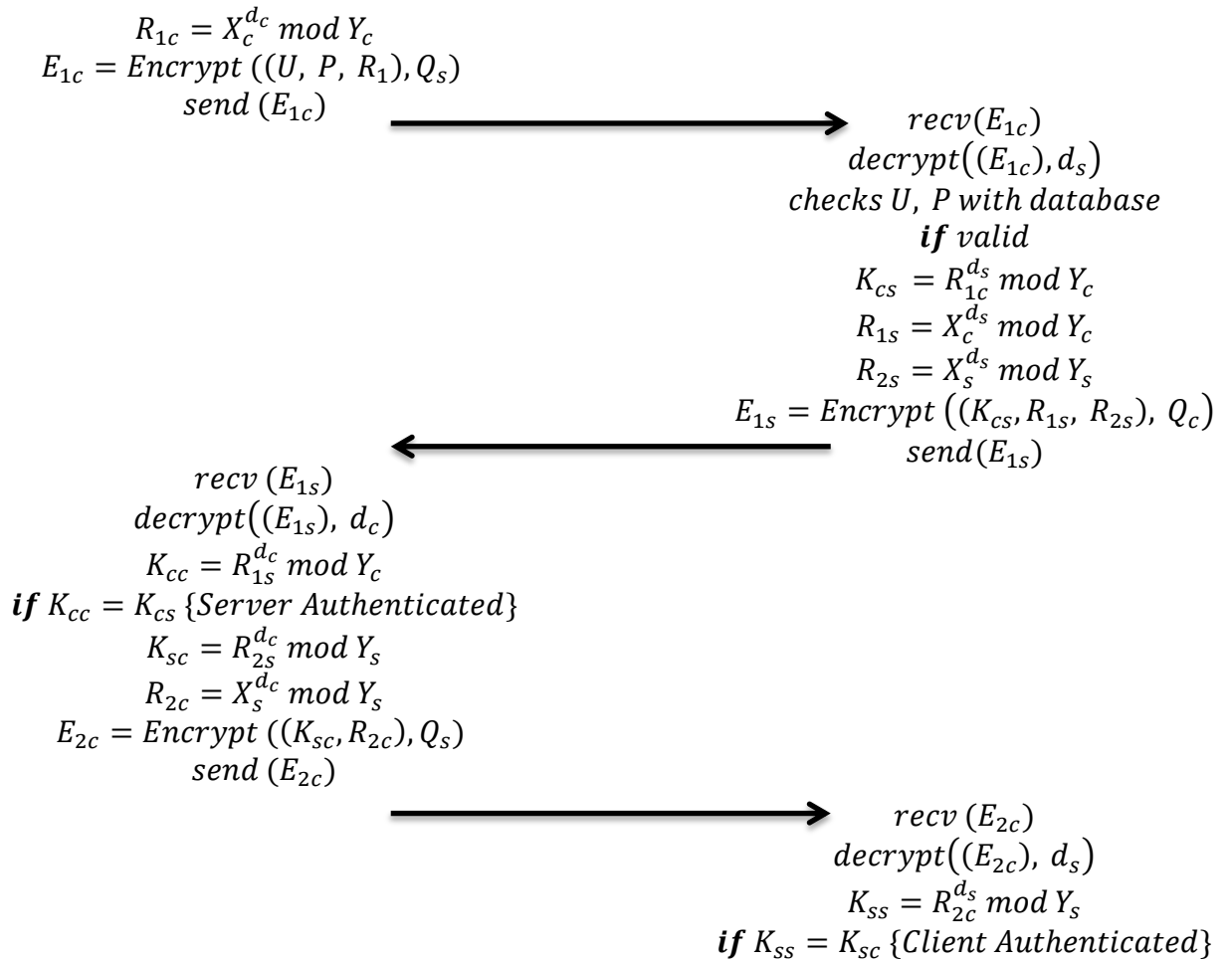
Research Methodology is the one of the important step in dissertation work. It includes all the steps of data collection, analyzing and important methodologies to provide results.

Security is the most important concern in cloud computing. Protecting data from unauthorized access is the main task while accessing cloud services. The technique provides authentication to users before entering into the cloud. The methodology includes two steps:

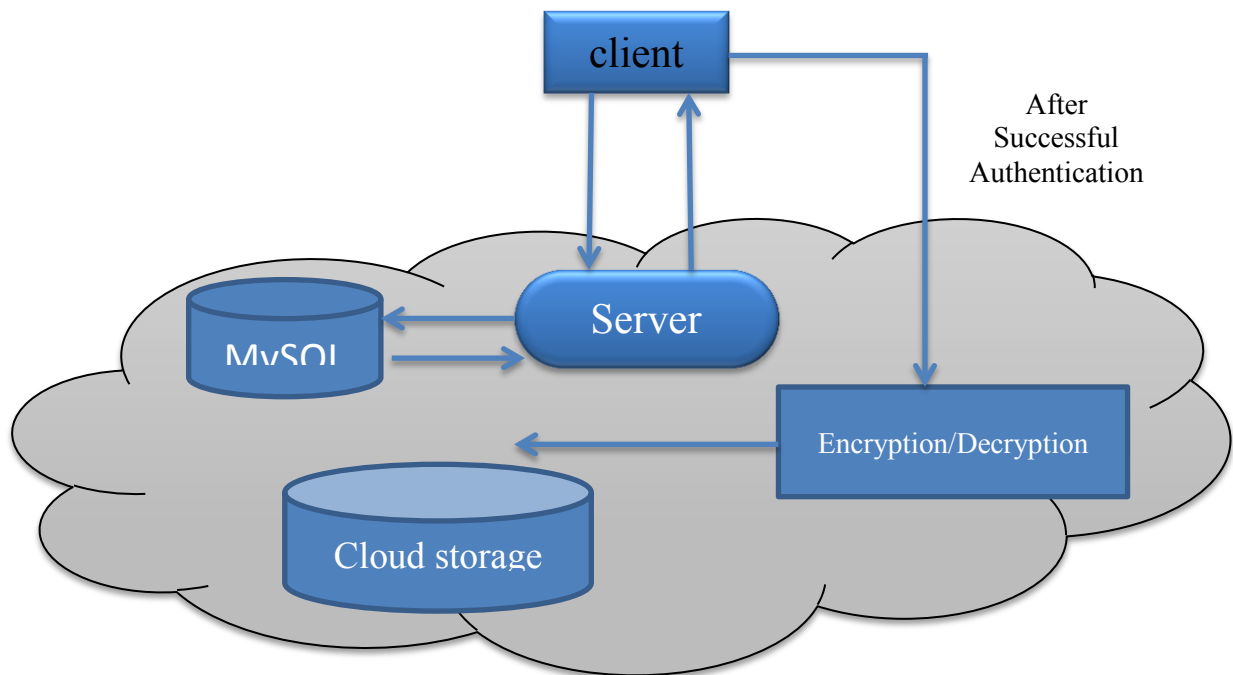
1) **Authentication:** It is the process of identifying a user. The authentication will be performed by Modified Diffie Hellmann agent. Earlier authentication was done from server side for client. Now authentication will be done for server too from client side which makes the communication more secure and results in secured cloud services. With this methodology authentication will become identifying not even user but server too. A cloud application called Authentication SaaS handles the process of authentication instead of mail cloud servers. After a successful authentication from both sides users will be allowed to access their data stored over a cloud and can store data over authenticated cloud. While authentication of users and server the whole communication will be done using elliptic curve cryptography which is proved to be better than RSA. Figure below shows the two way authentication from client and server. Q_c, d_c are the pair of public and private key of client side and Q_s, d_s are the pair of public and private key of server side. During the connection between server and client both will share their public key Q with each other so that the further communication between the two will be secured, both will now communicate with each other after encrypting data with the each other's public key and decrypt their own private key, d . At the client end username U , password P will be send along with the message R_{1c} which will be used to authenticate server. Rest of the steps is explained in the figure below.

Client $Q_c(X_c, Y_c), d_c$

Server $Q_s(X_s, Y_s), d_s$



2) **Encryption:** After successful completion of authentication between client and server, next step is for encrypting data before storing in the cloud. The encryption is done by cryptographic agent using elliptic curve cryptography algorithm. Whenever data is stored over cloud it will be encrypted using public key of client so that while accessing its own data only client can decrypt it. This approach makes the data more secure from attacks. The technique will be implemented by performing simulation using CloudSim simulator. The client accesses the services of cloud by login through a web application. The database used at the back end for storing the details of the client is MySQL. Figure below shows the steps after successful authentication of server and client.



3.5 Tools

- 1) ECILPSE is used for writing the code in accordance to our problem statement which implements our algorithm with each step intact.
- 2) The output will be displayed to the command window of ECILPSE console.

3.5.1 An Overview of ECILPSE Environment

Eclipse is an integrated development environment (IDE) for developing applications using the Java programming language and other programming languages such as C/C++, Python, PERL, Ruby etc.

The Eclipse platform which provides the foundation for the Eclipse IDE is composed of plug-ins and is designed to be extensible using additional plug-ins. Developed using Java, the Eclipse platform can be used to develop rich client applications, integrated development environments and other tools. Eclipse can be used as an IDE for any programming language for which a plug-in is available.

The Java Development Tools (JDT) project provides a plug-in that allows Eclipse to be used as a Java IDE, PyDev is a plugin that allows Eclipse to be used as a Python IDE, C/C++ Development Tools (CDT) is a plug-in that allows Eclipse to be used for developing application using C/C++, the Eclipse Scala plug-in allows Eclipse to be used an IDE to develop Scala applications and PHPEclipse is a plug-in to eclipse that provides complete development tool for PHP.

3.5.2 MySQL

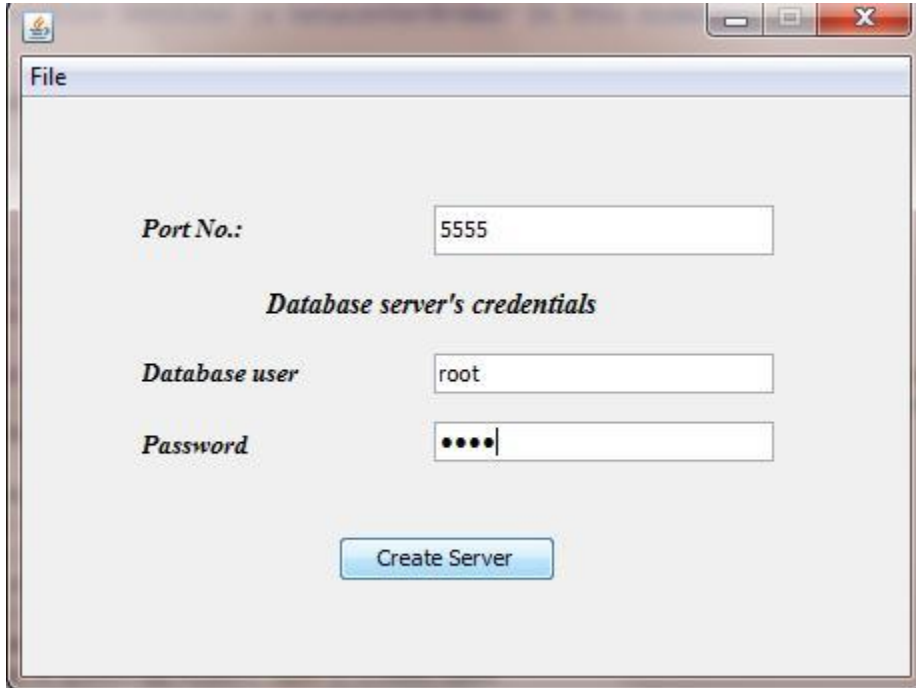
It is the world's most popular open source database. It is a Relational Database Management System (RDBMS) - data and its relationships are stored in the form of tables that can be accessed by the use of MySQL queries in almost any format that the user wants. MySQL is a fast, easy-to-use RDBMS used being used for many small and big businesses. MySQL is becoming so popular because of many good reasons.

- MySQL is released under an open-source license. So we have nothing to pay to use it.
- MySQL uses a standard form of the well-known SQL data language.
- MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA etc.
- MySQL works very quickly and works well even with large data sets.
- MySQL is very friendly to PHP, the most appreciated language for web development.

4.1 Implementation of the Proposed Technique

This part of the thesis discusses the overall performance and the result of the proposed scheme after implementation on the cloud environment. The whole implementation of the work proposed was done in JAVA language with eclipse as an Integrated Development Environment (IDE) and cloud-sim for simulation of the task submitted over the cloud. The whole implementation of the proposed scheme is based on the socket programming in java. We have created the client and server part which communicate with each other with encrypted messages. The MySQL database is installed on the server side to validate and register the user details. At the time of login it checks the validation of the user in the database

In ,Fig 3.1 Create Server: First of all , we create the server with specific port no. ,database user and password



File

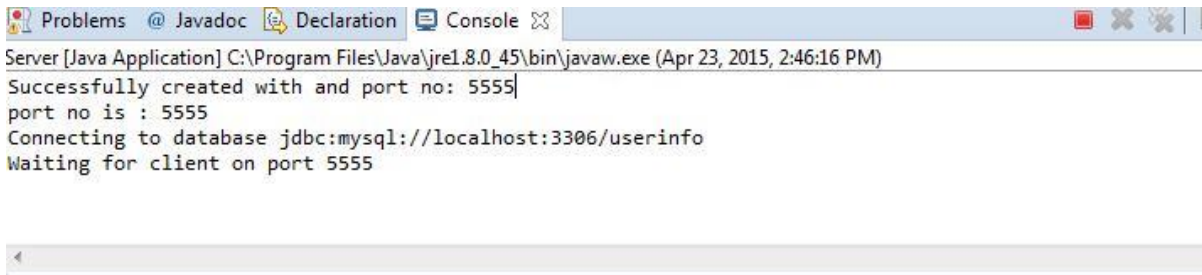
Port No.:

Database server's credentials

Database user

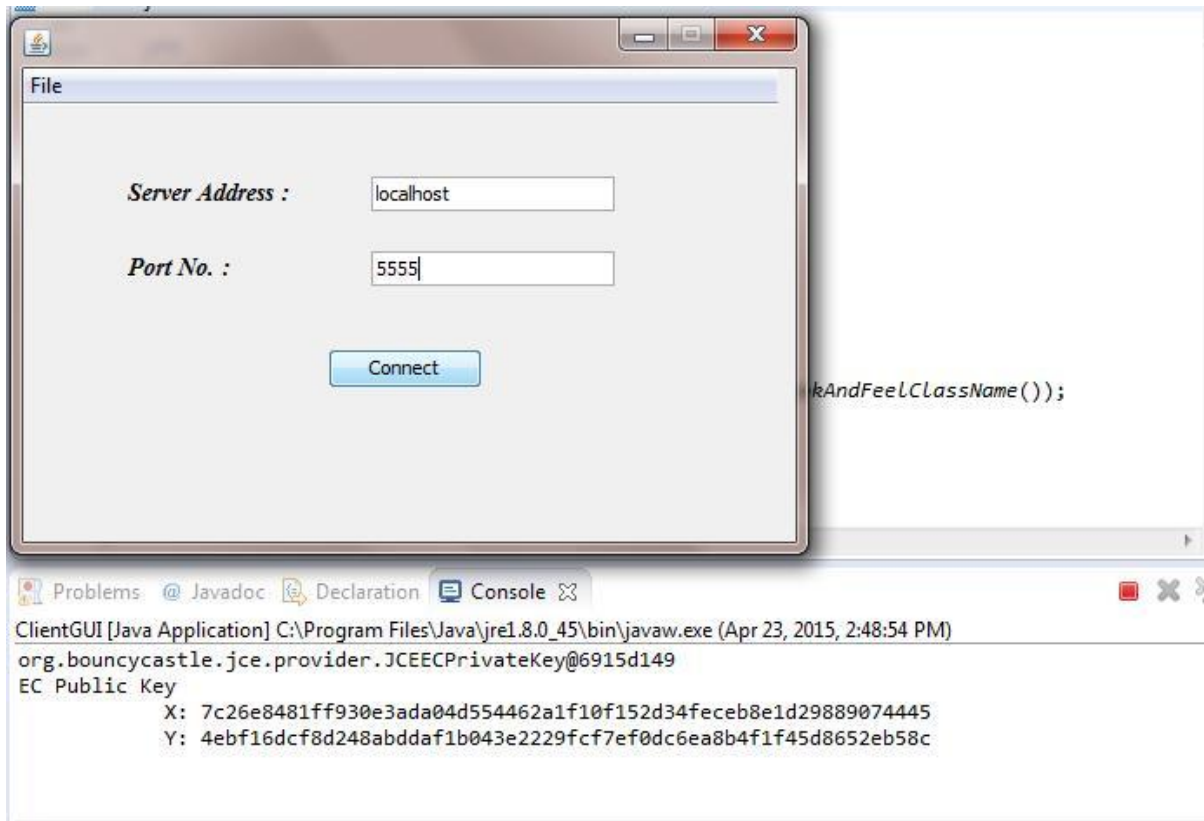
Password

After create the server, then server will wait for client

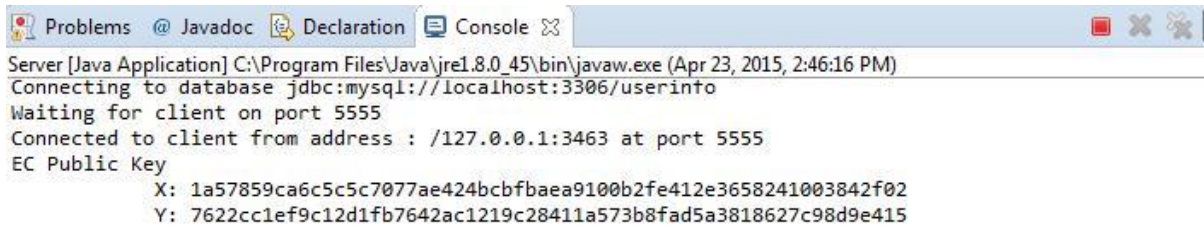


```
Problems @ Javadoc Declaration Console
Server [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (Apr 23, 2015, 2:46:16 PM)
Successfully created with and port no: 5555
port no is : 5555
Connecting to database jdbc:mysql://localhost:3306/userinfo
Waiting for client on port 5555
```

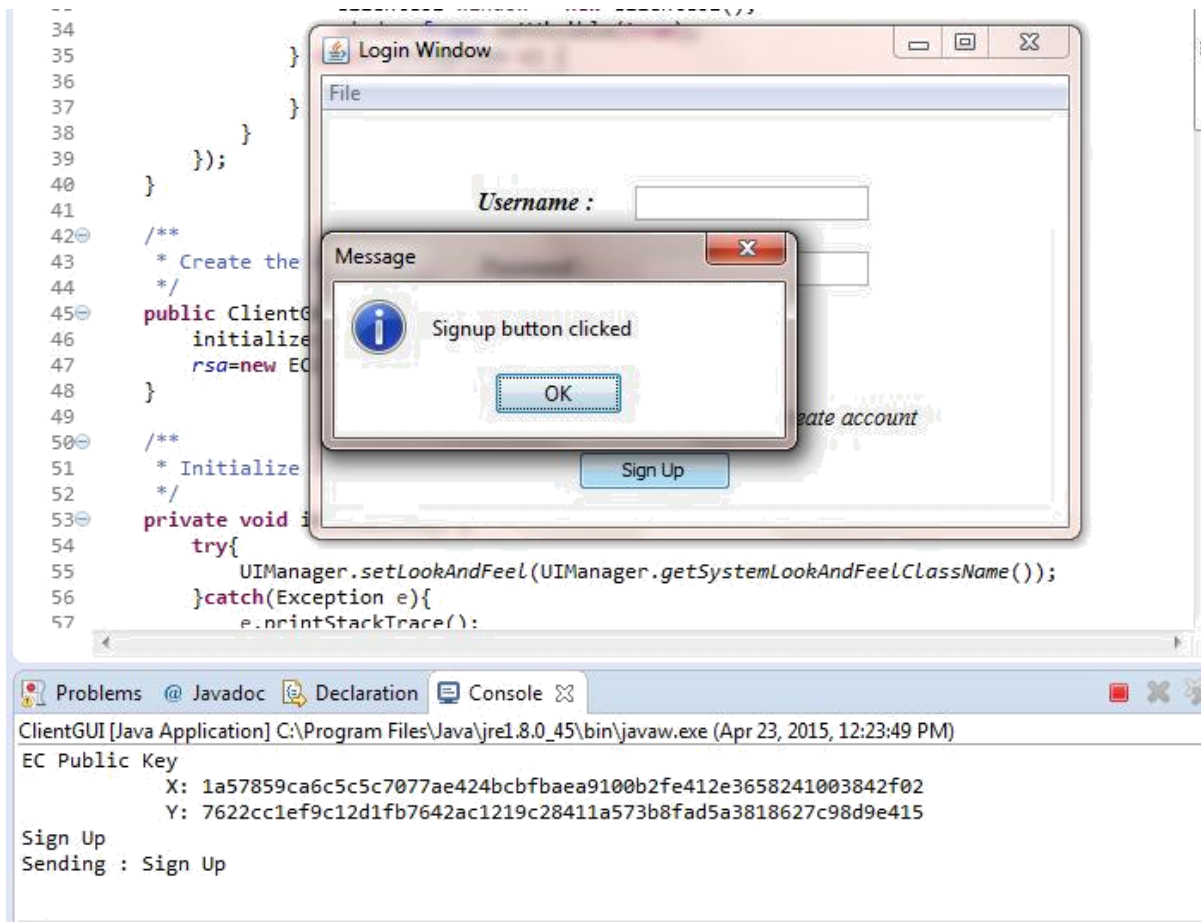
Connect to server: After create the server, then client connects with that created server



After successfully connected with server , message will shows as below:



Signup : After connected with server, now client will have to signup successfully. So that client will successfully authenticate to access the cloud services.



After clicking the signup, popup window will be open then fill up the details of the client.

Then finish ,click on add details

So that user can able to access the cloud services.



Result will show as below

```
Sign Up
Sending : Sign Up
Add Details
Sending : Add Details
nav
Sending : nav
1-9-90
Sending : 1-9-90
F
Sending : F
nav
Sending : nav
0987
Sending : 0987
Details added
```

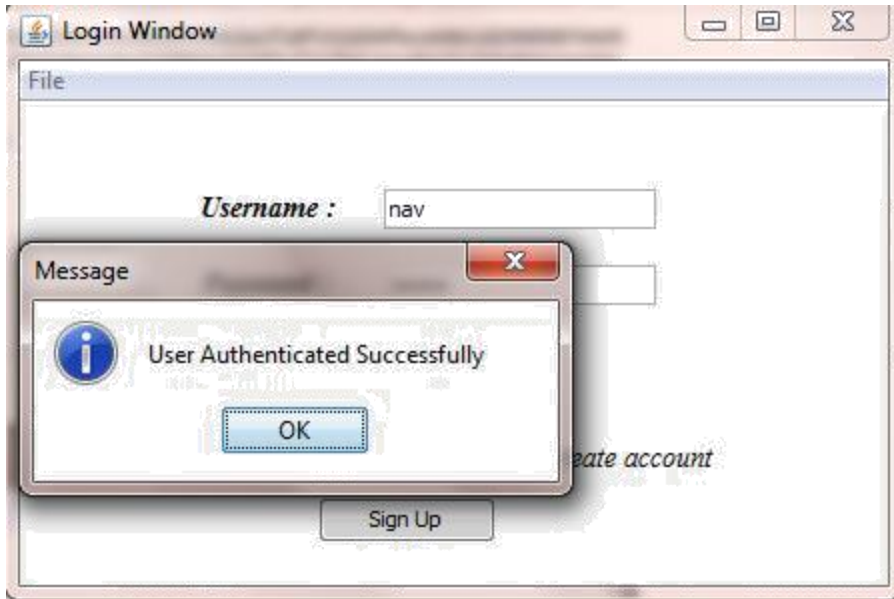
On server side , all the details will be received successfully. And stored in the database

```
Problems @ Javadoc Declaration Console
Server [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (Apr 23, 2015, 2:46:16 PM)
EC PUBLIC key
    X: 7c26e8481ff930e3ada04d554462a1f10f152d34feceb8e1d29889074445
    Y: 4ebf16dcf8d248abddaf1b043e2229fc7ef0dc6ea8b4f1f45d8652eb58c
Receiving : Sign Up
Sign Up
Receiving : Add Details
Signing up
Receiving : nav
Receiving : 1-9-90
Receiving : F
Receiving : nav
Receiving : 0987
nav 1-9-90 F nav 0987
```

Login : After successfully signup, we can now login to access the files.



After login, user will authenticate successfully



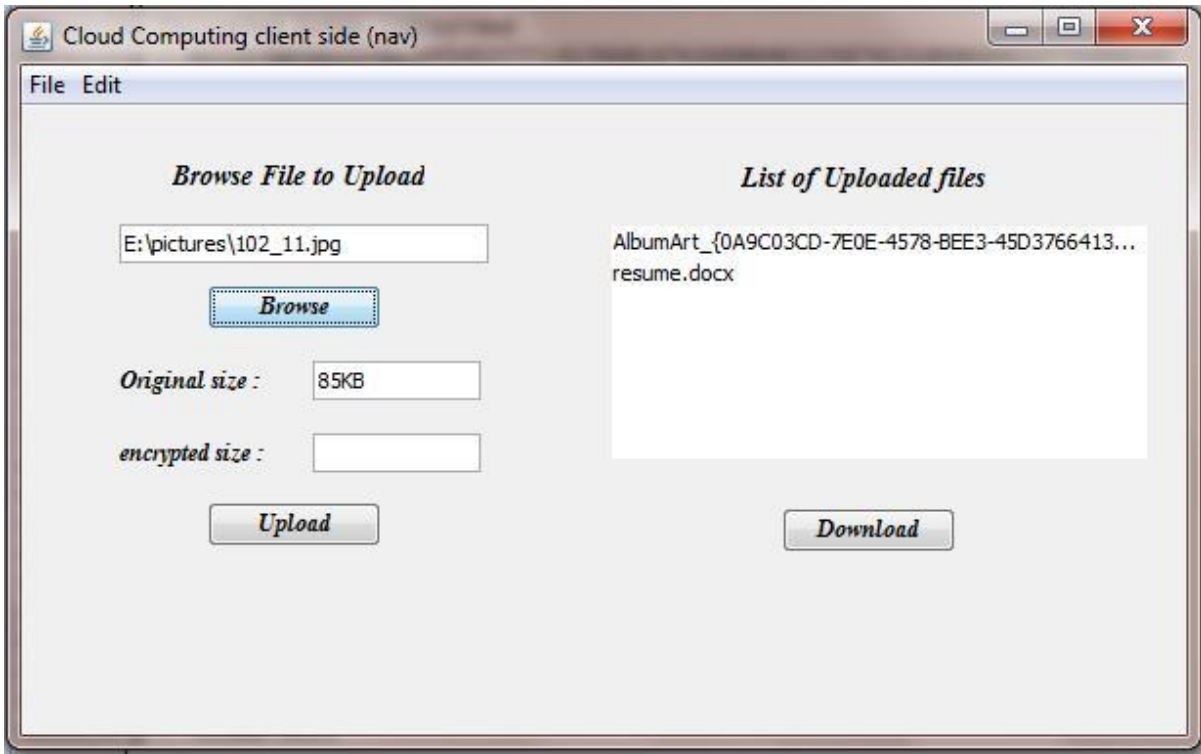
After login, server and client both are authenticate successfully.

```

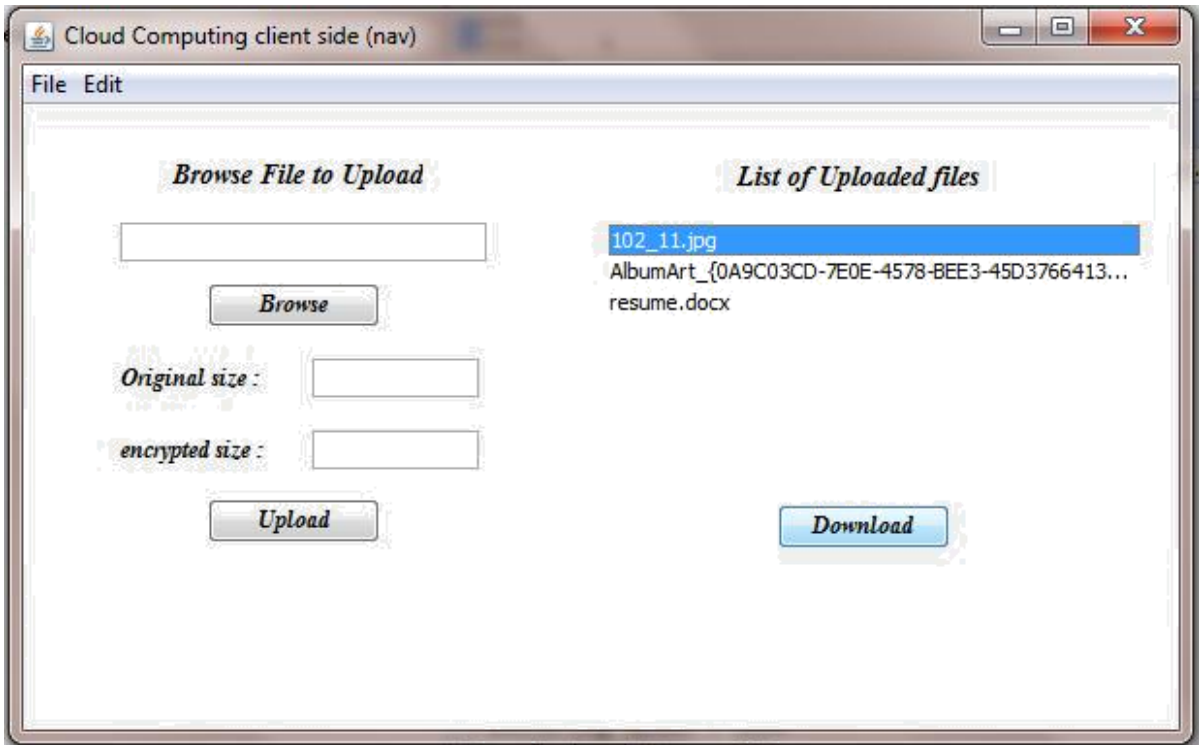
Problems @ Javadoc Declaration Console
ClientGUI [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (Apr 23, 2015, 2:48:54 PM)
Login
Sending : Login
nav
Sending : nav
0987
Sending : 0987
Sending : 533497584072854165187882934264500086264373262292289179385837543646796733
533497584072854165187882934264500086264373262292289179385837543646796733
Sending : 533497584072854165187882934264500086264373262292289179385837543646796733
this is client sode message
Sending : this is client sode message
Receiving Encrypted bytes [B@e4f5d5
Receiving : valid
Receiving Encrypted bytes [B@686b2b
Receiving : 359796532864963921581977190187835973840344602167859672063241390849043345
Receiving : 359796532864963921581977190187835973840344602167859672063241390849043345
Receiving Encrypted bytes [B@1874acb
Receiving : 457157005861576629554537771413960147626880402225874131060684622735080141
Receiving : 457157005861576629554537771413960147626880402225874131060684622735080141
Receiving Encrypted bytes [B@b834e1
Receiving : 343807023226967530958713728745880841096439070803459516119939841693853592
Receiving : 343807023226967530958713728745880841096439070803459516119939841693853592
Valid user
server verified
Sending : server verified
Sending : 85381540135385914720703991302226457935086032900814940009678128778793185
85381540135385914720703991302226457935086032900814940009678128778793185
Sending : 85381540135385914720703991302226457935086032900814940009678128778793185
Sending : 348919092780094133725328579017882851100061627361635784852388494630868803
348919092780094133725328579017882851100061627361635784852388494630868803
Sending : 348919092780094133725328579017882851100061627361635784852388494630868803
Receiving Encrypted bytes [B@1943c6e
Receiving : Authenticated
User Successfully Logged in

```

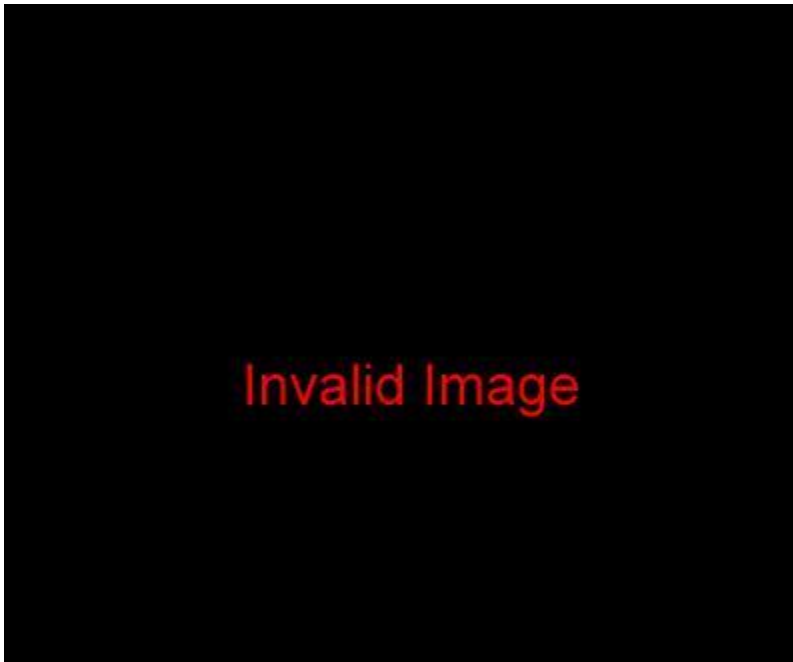

Now user can upload the file on cloud. When we upload the file, that file first of all encrypt then store in cloud. So that any intruder doesn't harm the upload file.



After upload the file in cloud, now user can download his/her file . but first of all he/she have to authenticate then he /she will download file easily. When we are download the file, first of all decrypt that encrypted stored file .



Every file that are uploaded into cloud , first of all encrypted then store in the cloud and when you want to download the file that file first decrypt so user can access safely. If any attacker access that file on cloud, then they will see nothing. As below image:



It will take 0.641 secs to authenticate the client and server.

```
Problems @ Javadoc Declaration Console
Server [Java Application] C:\Program Files\Java\jre1.8.0_45\bin\javaw.exe (Apr 23, 2015, 2:46:16 PM)
Receiving : Login
Login\
Receiving : nav
Receiving : 0987
Receiving : 533497584072854165187882934264500086264373262292289179385837543646796733
Receiving : 533497584072854165187882934264500086264373262292289179385837543646796733
Receiving : this is client sode message
0987
Sending : valid
Sending : 359796532864963921581977190187835973840344602167859672063241390849043345
Sending : 359796532864963921581977190187835973840344602167859672063241390849043345
Sending : 457157005861576629554537771413960147626880402225874131060684622735080141
Sending : 457157005861576629554537771413960147626880402225874131060684622735080141
Sending : 343807023226967530958713728745880841096439070803459516119939841693853592
Sending : 343807023226967530958713728745880841096439070803459516119939841693853592
Receiving : server verified
Receiving : 85381540135385914720703991302226457935086032900814940009678128778793185
Receiving : 85381540135385914720703991302226457935086032900814940009678128778793185
Receiving : 348919092780094133725328579017882851100061627361635784852388494630868803
Receiving : 348919092780094133725328579017882851100061627361635784852388494630868803
Sending : Authenticated
Total time for authentication: 0.641secs
creating directory: nav
DIR created
Sending list of files in the directory
Sending : 0
```

In the implementation of the scheme we used the elliptic curve cryptography which is well proved to be difficult problem to break or find keys to decrypt messages. The solution to find these keys are under discrete logarithmic which is NP hard problem. So there is no doubt in the decryption of the messages from attacker.

The second part is the total time taken over the complete task of two way authentication. The results of the mention task are shown in Table below. The time taken for the authentication is performed over the different key size using elliptic curve cryptography. As it performs the two way authentication, so it is obvious that it will take more time as compared to the other approach. But the time to generate Big prime number for encrypting message for mutual authentication is overcome by using X and Y co-ordinates of public key of ECC.

Key Size	Execution Time (milliseconds)
64	200-204
128	220-225
256	235-240
512	256-260

After successful completion of the user and server authentication, users are allowed to access or store their data in the encrypted form and download it after decryption of the same. The result for encryption and decryption over the cloud for different file size and key size of public and private key in ECC is shown in table below. The operation is performed over the two file of size 22 bytes and 28242 bytes respectively.

It also shows the size of the file after encryption of it and same for the decryption.

Key Size	File size before Encryption (in bytes)	Encryption Time (milliseconds)	File size after Encryption (in bytes)	Decryption time (milliseconds)	File size after Decryption (in bytes)
64	22	16	42	16	22
	28242	62	28262	62	28242
128	22	18	42	18	22
	28242	63	28262	63	28242
256	22	20	42	20	22
	28242	50	28262	50	28242
512	22	11	42	11	22
	28242	48	28262	48	28242

Hence the proposed scheme is much secure with the little expense of the time taken to authenticate which is reasonable for it.

Conclusion and Future Scope

4.1 Conclusion and future scope:

Two way authentication scheme is a new approach for cloud environment which no doubt provides the better and secure communication between server and client and hence allow user to connect with storage space or cloud services after passing through the much secured way of authentication. This authentication scheme not only authenticates client or user but also authenticates server to the client before providing dedicated link to user to its storage space / cloud services. As compared to dual RSA encryption for authentication it requires a generation of two random big prime numbers which is avoided in our case since ECC provides the public key with the combination of the coordinates so we can use those coordinates instead of G and P as mentioned in the authentication using RSA. ECC also provides better security as compared to RSA with small key size with respect to the key size of RSA.

It has been theoretically proved that ECC is much harder to break as compared to RSA since it is discrete logarithmic problem which takes it to NP-hard problem. So decrypting any messages encrypted by ECC algorithm is much difficult as compared to others. So we had implemented the data encryption uploaded by user using ECC at the server end and decryption of the same will be implemented at the client end since only client knows the private key to decrypt it, which cannot be shared with others.

For future references this task of two way authentication can be performed with different upcoming cryptographic algorithm which will be better than ECC as the research in the area of cryptography is becoming deeper which will results in better cryptographic algorithm.

REFERENCES

- [3] <http://www.datahouse.com/assets/files/Cloud-1.0.pdf>
- [4] http://www.opengroup.org/cloud/cloud/cloud_for_business/image003.jpg
- [5] <http://www.smartcloud.ie/cloud-computing.html>
- [6] FarazFatemiMoghaddam and SohrabRouzbeh, " A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments," Region 10 Symposium, IEEE, April 2014, pp. 508 - 513.
- [7] Bhavana Sharma, "Security Architecture Of Cloud Computing Based On Elliptic Curve Cryptography (ECC)," in Proceedings of 2nd International Conference on Emerging Trends in Engineering and Management, ICETEM 2013, pp. 58-61.
- [8] VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography," International Journal of Soft Computing and Engineering (IJSCE), vol. 2, pp. 138-141, July 2012.
- [9] Chen, D., & Zhao, H., "Data Security and Privacy Protection issues in Cloud Computing," In Proceedings of International Conference of Computer Science Electronics Engineering(ICCSEE), Hongzhou: IEEE, 2012 , pp. 647-651.
- [10] Pragnesh G. Patel, S.M.Shah, "Data Security in Cloud Computing using Elliptical Curve Cryptography," International Research Journal of Computer Science Engineering and Applications, vol. 2, pp. 479-483, July 2013.

