Deployment of Application on Cloud and Enhanced Data Security in Cloud Computing using ECC Algorithm

Neha A Puri[1], Ajay R Karare[2],Rajesh. C. Dharmik[3]
[1,2]Department of IT,YCCE, Nagpur, Maharshtra, India
[3]Department of CSE,JDCOEM, Nagpur, Maharashtra, India
[1]neha.puri100@gmail.com,[2] ajju.karare@gmail.com,[3]raj_dharmik@yahoo.com

Abstract—**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. Scalibility 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 major 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 Paper will explore the deployment of Application on the Cloud and increases the security level by implementing ECC Algorithm,Digital Signature and Encryption.**

Keywords— Elliptic Curve Cryptography, Encryption Algorithms, Types of services in Cloud Computing, Cloud Security, Encryption.

I INTRODUCTION

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[1]. The services in Cloud Computing are SaaS, PaaS, IaaS amongst which we are using PaaS and IaaS 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 the their priority[6]

These security parameters are achieved due to which the performance will gets increased and therefore the Security is obtained upto higher extent.

Data security and privacy risks have become the primary concern for people to shift to cloud computing [1].

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 [1]

Cloud is the free space where the application is being saved securely and the services are being provided continuously when and where required

II DEPLOYMENT CLOUD 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.

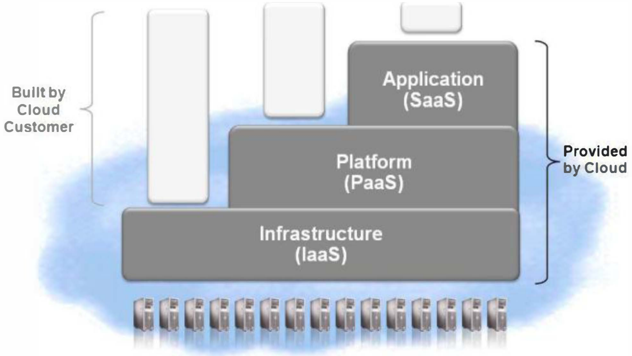


Fig.1. Service Model

III CLOUD CHARACTERISTIC

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.

IV DEPLOYMENT OF APPLICATION ON CLOUD

The Application which is being created has two users one is Admin and other is General User.

Admin will be able to Add, Modify, Delete, Upload and can view the data. This Paper satisfies with three security parameters such as Authentication, Encryption and Separation of Duties. Authentication is used to provide the identity of the particular user which requires creating the user id and password. For the Deployment of Application on the Cloud will have to follow certain steps.

V CHALLENGES AND SECURITY ISSUES

There are many Security issues in Cloud Computing which occurs mostly during the time of transmission of data .Some of the Security issues 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 [3].

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

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

VI DATA PRIVACY IN CLOUD

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[5]. 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.

A *Public Key Cryptography*- In this cryptography different keys are used for Encryption and Decryption.

B *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 beastest Algorithm which is having the high level of Security and better performance.

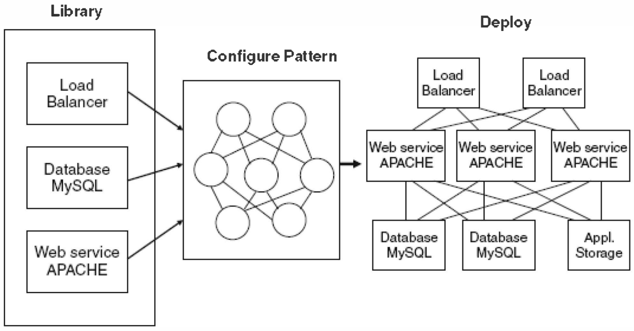


Fig.2. Deployment Strategy on Cloud for two tier architecture

VI ELLIPTIC CURVE CRYPTOGRAPHY

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 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?

VII. NECESSARY CONDITIONS FOR ENCRYPTION IN ELLIPTIC CURVE

1) Discriminant of a Polynomial is the product of the squares of the differences of the polynomial roots.
2) The Discriminate must not become zero
3) It is not safe to use singular curves for
4) Elliptic Curve in their standard form will be Symmetric [5]

VIII. PROPOSED SYSTEM: ECC ALGORITHM

There are many security parameters will are used to make the system more secure. For the implementation of ECC Algorithm we consider here basically three Security parameters such as Authentication, Separation of Duties and Encryption for Secure transmission of data. In order to satisfy the above mentioned three security parameters will have to adopt the following steps.

A. Key Agreement

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[4].

1)A will select an integer XA = k1as his/her private key. The public key for A will be YA = XA × 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 ×P. Then both the parties exchange their public keys.

3) A computes the session key by

KA = XA×YB = k1×k2×P

4) B computes the session key by

KB = XB×YA = K2×k1×P.

Obviously, KA = K

This proves the Agreement for exchanging the Data between two parties and the generation of public and private key[4].

B. Key Generation

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

C. 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 takes place and for the transmission of data only few nano seconds will be required to travel the data to receiver.

IX RESULTS

Following are the steps will be followed for the deployment of Application on cloud they are:

Step 1) First will have to create the Environment and select the tools that we required

- Apache Tomcat 7.0.39
- Java 7.0
- MySQL 5.5.32

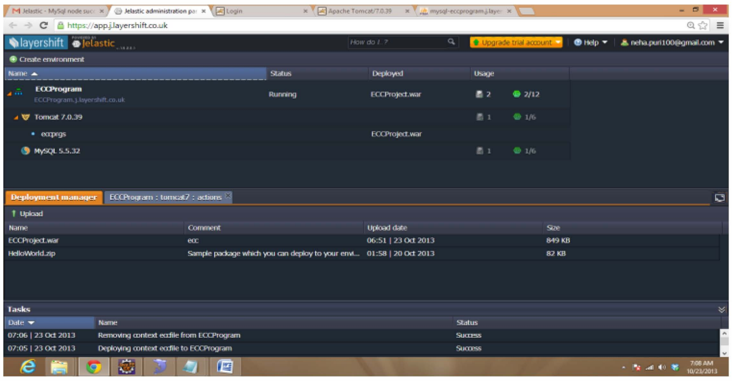
Step 2) Create the WAR file of the Project which is imported in the Eclipse.

Step 3) Upload a WAR file of project on the Cloud.

Step 4) Deploy the WAR file on the cloud.

Step 5) Deploy the WAR file on to the Cloud Environment.

While creating the cloud Environment will have to go to the cloud link where we get the particular cloud will have to select the cloudlets i.e the amount of space on the Cloud. As we are developing our project in JAVA using the Eclipse in that the we had created a project of which we are creating a WAR file and then will deploy it on the cloud.



Name	Status	Deployed	Usage	
ECCProgram ECCProgram.j.layershift.co.uk	Running	ECCProject.war	2	2/12
Tomcat 7.0.39			1	1/6
eccprgs		ECCProject.war		
MySQL 5.5.32			1	1/6

Name	Comment	Upload date	Size
ECCProject.war	ecc	06:51 | 23 Oct 2013	849 KB
HelloWorld.zip	Sample package which you can deploy to your envi...	01:58 | 20 Oct 2013	82 KB

Tasks

Date	Name	Status
07:06 | 23 Oct 2013	Removing context eccfile from ECCProgram	Success
07:05 | 23 Oct 2013	Deploying context eccfile to ECCProgram	Success

Fig.3. Cloud Environment

A. User Login

Log in to the Jelastic cloud portal using your live id to deploy the application on the cloud.

This is the Login Page of the Application where the user has to enter his User ID and Password. If the user is new then he will has to follow the Registration process as per the rules and regulations of the registration process. After registration user details will be stored in the Database .New user will be able to logged in only when the Verification is to be done. If the User is Authenticated then only he will be able to logged in to the system.

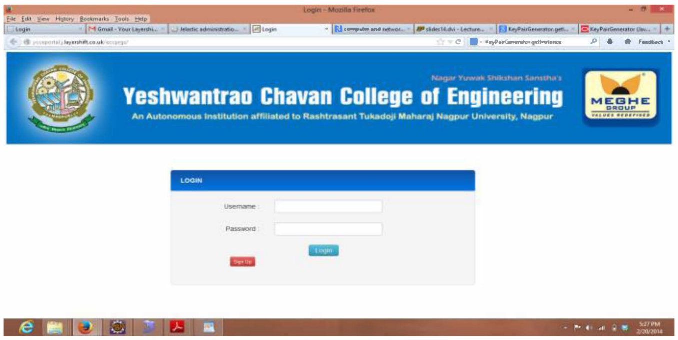
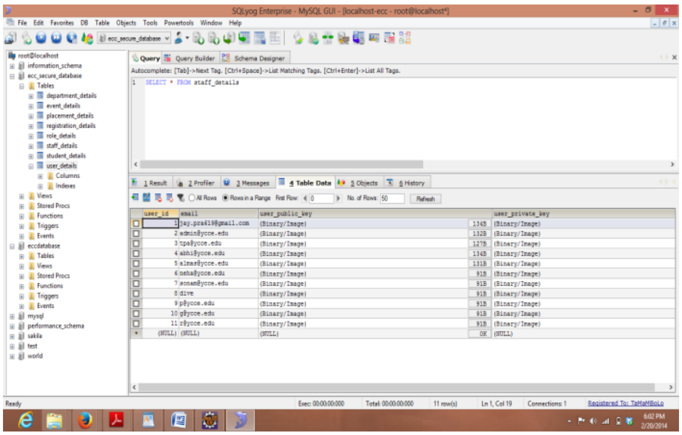

Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Login
Gmail - Your Layershi...
Jelastic administratio...
Login
computer and networ...
slides14.dvi - Lecture...
KeyPairGenerator.get...
KeyPairGenerator (Jav...
Feedback
Nagar Yuwak Shikshan Sanstha's
Yeshwantrao Chavan College of Engineering
An Autonomous Institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
MEGHE GROUP
LOGIN
Username :
Password :
Login
Sign Up
5:27 PM
2/20/2014

Fig.4. User Login

B. Digital Signature Generation

Digital Signature is used to maintain the Integrity and it is mostly used to generate by the sender in order to sign the document to ensure that the document which is send by the sender is an original and send by the original sender only. The Data which is being send by the sender is being encrypted by using the digital signature which uses the hash Algorithm called as SHA 1.

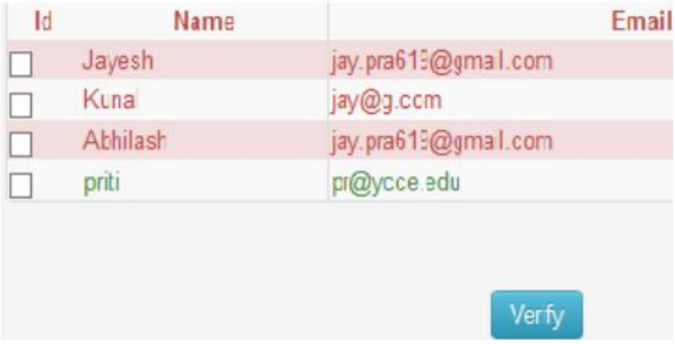


```
SELECT * FROM staff_details
```

user_id	email	user_public_key		user_private_key
1	jay.pra619@gmail.com	(Binary/Image)	134B	(Binary/Image)
2	admin@ycce.edu	(Binary/Image)	132B	(Binary/Image)
3	tpa@ycce.edu	(Binary/Image)	127B	(Binary/Image)
4	abhi@ycce.edu	(Binary/Image)	134B	(Binary/Image)
5	almas@ycce.edu	(Binary/Image)	131B	(Binary/Image)
6	neha@ycce.edu	(Binary/Image)	91B	(Binary/Image)
7	sonam@ycce.edu	(Binary/Image)	91B	(Binary/Image)
8	dive	(Binary/Image)	91B	(Binary/Image)
9	p@ycce.edu	(Binary/Image)	91B	(Binary/Image)
10	g@ycce.edu	(Binary/Image)	91B	(Binary/Image)
11	r@ycce.edu	(Binary/Image)	91B	(Binary/Image)
(NULL)	(NULL)	(NULL)	0K	(NULL)

Fig.5. Digital Signature Generation

After the generation of Digital Signature it is being verified. If any of the third person will used to modify the data then we will came to know about the modification with the help of messages displayed on the screen as violated and verified.

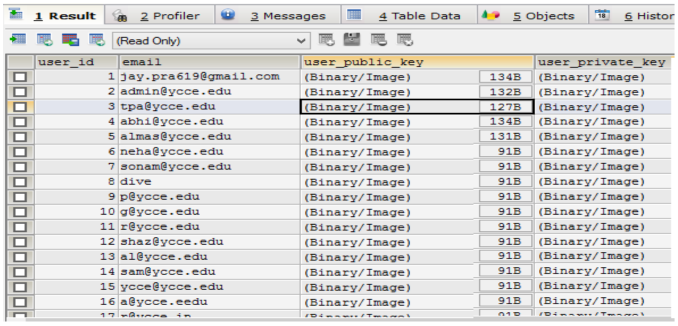


Id	Name	Email
□	Jayesh	jay.pra61?@gma l.com
□	Kuna	jay@j.ccm
□	Abhilash	jay.pra61?@gma l.com
□	priti	pr@ycce.edu

Fig.6. Digital Signature Verification

C. Key Generation

A Key pair is being generated. For each and every user a separate private and public key is being generated. The key generation time is different even though the key length is same. It takes the very less time for generation of key having the smaller key size.

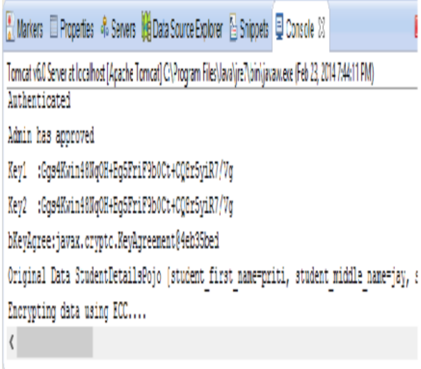


user_id	email	user_public_key		user_private_key
1	jay.pra619@gmail.com	(Binary/Image)	134B	(Binary/Image)
2	admin@ycce.edu	(Binary/Image)	132B	(Binary/Image)
3	tpa@ycce.edu	(Binary/Image)	127B	(Binary/Image)
4	abhi@ycce.edu	(Binary/Image)	134B	(Binary/Image)
5	almas@ycce.edu	(Binary/Image)	131B	(Binary/Image)
6	neha@ycce.edu	(Binary/Image)	91B	(Binary/Image)
7	sonam@ycce.edu	(Binary/Image)	91B	(Binary/Image)
8	dive	(Binary/Image)	91B	(Binary/Image)
9	p@ycce.edu	(Binary/Image)	91B	(Binary/Image)
10	g@ycce.edu	(Binary/Image)	91B	(Binary/Image)
11	r@ycce.edu	(Binary/Image)	91B	(Binary/Image)
12	shaz@ycce.edu	(Binary/Image)	91B	(Binary/Image)
13	al@ycce.edu	(Binary/Image)	91B	(Binary/Image)
14	sam@ycce.edu	(Binary/Image)	91B	(Binary/Image)
15	ycce@ycce.edu	(Binary/Image)	91B	(Binary/Image)
16	a@ycce.eedu	(Binary/Image)	91B	(Binary/Image)
17	r@ycce.in	(Binary/Image)	91B	(Binary/Image)

Fig.7. Key Generation

D. Key Agreement

When both the parties will ready to transmit the data at a point then only the data will gets transmitted..

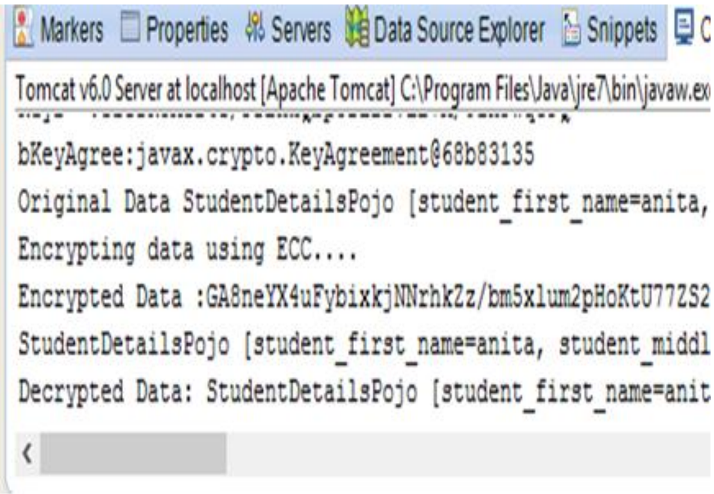


```
Tomcat v6.0 Server at localhost [Apache Tomcat] C:\Program Files\Java\jre7\bin\javaw.exe (Feb 23, 2014 7:44:11 PM)
Authenticated

Admin has approved

Key1  :Ggs4Kwin48NqOH+Eg5FriF9b0Ct+CQ6r5yiR7/Vg

Key2  :Ggs4Kwin48NqOH+Eg5FriF9b0Ct+CQ6r5yiR7/Vg

bKeyAgree:javax.crypto.KeyAgreement@4eb35bed

Original Data StudentDetailsPojo [student_first_name=priti, student_middle_name=jay, s

Encrypting data using ECC....
```

Fig.8. Key Agreement

E. Encryption

Encryption is used to encode the original message so the third party will not be able to get the message send by the sender. Let m be the message that has been sent by the sender A to B. Sender A will encode the message and the data is transmitted towards the receiver. On the way during the transmission only the data is being encrypted. It takes very less time to encrypt the data i.e. few nano seconds will be required to transmit the encrypted data. After comparing the Execution time for the Encryption of different Algorithms such as AES, DES, RSA and Blowfish. We found that the speed of ECC Algorithm is twice times to the speed of DES and RSA Algorithm



```
Tomcat v6.0 Server at localhost [Apache Tomcat] C:\Program Files\Java\jre7\bin\javaw.ex
bKeyAgree:javax.crypto.KeyAgreement@68b83135
Original Data StudentDetailsPojo [student_first_name=anita,
Encrypting data using ECC....
Encrypted Data :GA8neYX4uFybixkjNNrhk2z/bm5xlum2pHoKtU77ZS2
StudentDetailsPojo [student_first_name=anita, student_middl
Decrypted Data: StudentDetailsPojo [student_first_name=anit
```

Fig..9. Encryption and Decryption

X CONCLUSION

Now a day‘s users are concerned more about the security of data as the data which is being transferred from one cloud to another cloud. Elliptic curve cryptography provides the higher level of security and performance is also much better than other encryption Algorithms. We concern about the higher level of security and therefore we proposed ECC Algorithm which takes least amount of time to encrypt the data .There are three security parameters such as Authentication, Encryption and Separation of Duties for the security has been satisfied which helps us to achieve the higher level of security. The presented simulation results showed that ECC is more secure and has the better performance than other Encryption Algorithms. Future work is to newly propose a more secured system in which if thes unregistered user will access the data must be blocked from entire network. A Proxy Re-encryption scheme and also the parameters of higher bits which satisfy the ECC Algorithm has been taken into consideration for providing higher security of data.

REFERENCES

[1] N. Ram Ganga Charan, S. Tirupati Rao, Dr .P.V.S Srinivas Deploying an Application on the Cloud|| International Journal Advanced Computer Science and Applications, Vol. 2, No. 5, 2011

[2] DeyanChen , Hong Zhao —Data Security and Private Protection Issues In Cloud Computing||2012 International Conference on Computer Science and Electronics Engineering

[3] Qi Zhang · Lu Cheng · RaoufBoutaba|| Cloud computing: state-of the-art and research challenges|| InternetServAppl (2010) 1: 7–18

[4] EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, Enhanced Data Security Model for Cloud Computing The 8th International Conference on Informatics and System (INFOS2012)- 14-16 May

[5] N. Jenefa, J. Confidentiality and Data Forwarding International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231 2307, Volume-3, Issue-1, March-2013

[6] A.P.Nirmala, Dr. R. Sridaran —Cloud Computing Issues at Design and Implementation Levels – A Survey|| Int. J. Advanced Networking and Applications Volume :03 Issue:06 Pages:1444-1449 (2012) ISSN :0975-0290

[7] Ramgovind S, Eloff MM, Smith E —The Management of Security in Cloud Computing|| 978-1-4244-5495- 2/10/$26.00 ©2010 I

[8] Introduction to the cloud computing architecture white paper 1st edition 2009 by sun Microsystems

[9] Mohsin Nazir — Cloud Computing: Overview & Current Research

[10] VeerrajuGampala, SrilakshmiInuganti, SatishMuppidi Data Security in Cloud Computing with Elliptic Curve Cryptography "International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-3, July 2012

[11] YouryKhmelevsky, VolodymyrVoytenko —Cloud Computing Infrastructure Prototype for University Education and Research WCCCE '10, May 7–8, 2010,Kelowna, Canada

[12] D. L. Ponemon, "Security of Cloud Computing Users"