International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12-13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

Deployment of Application and Review of Different Encryption Algorithm for Cloud Computing

Mr. Ajay R Karare, Ms. Neha A Puri, Prof.M.M.Baig
Department of CSE, Nagpur University, Nagpur
Department of Information Technology, Nagpur University, Nagpur

ABSTRACT-
Security in the Cloud Computing is an vital issue and it is an most evolving area and it is very much accepted by most of the organization. There are number of services available in Cloud Computing with the help which we can develop and deploy our own application on the Cloud and also can store all the valuable data on the Cloud, as well we can acess that application and stored data from anywhere in the world with the simple inetrnet connection. Basically we have to take care of the security by encrypting our data before it is being stored on the Cloud. For this purpose we will be using ECC Algorithm in our project after comparing many Encryption Algorithms, because of its advantages in terms of CPU time utilization, time for Encryption, memory usage and key size. Our paper determines the technique for providing the privacy and security in Cloud Computing along with the Deployment of the application on Cloud.
Keywords - Elliptic Curve Cryptography, Encryption Algorithms, Types of services in Cloud Computing, Cloud Security, Encryption

I. INTRODUCTION

A cloud is a virtualized pool of resources which are relocated for different purposes. Cloud Computing is a concept which is used to deliver the services and the resources continuously when and where required. The core concept of Cloud Computing is to improve the data handling capability. All of this is available through a simple Internet connection. Cloud Computing is used to reduce the processing burden on the user's terminal. Through Cloud Computing clients can access standardized IT resources to deploy the application on the Cloud**.**

Fig 1: Cloud Storage

Now a day's Cloud Computing is in great demand in various fields such as Scientific, Business, Medical etc. Also cloud is used very widely for educational Institute purpose in order to store the college data and on the cloud. [2]

To secure the data systems use the combination of techniques such as:

- Encryption- Is used to encode the Information so that no one will able to hack the data.
- Authentication- Is one of the Security parameter creating user id and password.
- Separation of duties- In which accessibility is provided to all the users according to the their priority[6]

II. CLOUD COMPUTING SUB SERVICE MODEL

Services provided by cloud computing can be split into three major categories:

A. Software as a Service (SaaS): This services are Applications over Internet e.g. Google Docs.The provision of an application which is hosted (off premise) by a provider as a service to customers who access it via the Internet. In contrast to application service providing (ASP), SaaS is based on a multi tenant model where many customers are using the same program code but have their own private data spaces. SaaS does not require much customization or integration with other applications

B. Platform as a Service (PaaS): This service provides platform for deploying the application on the Cloud. All The lifestyle for the deployment of application such as design, implementation, deployment etc included in this service. The provision of resources required to build applications and services (software development environment) to a customer by an outsourcing provider. Typical use scenarios are application design, development, testing and deployment.

C. Infrastructure as a Service (IaaS): Computer infrastructure is being offered by this service. It delivers a platform virtualization environment as a service rather than purchasing server, software, data centers. The provision of computing resources to a customer by an outsourcing provider. In this service model it is possible to share a server among multi tenants. The service is typically billed on a utility computing basis (resource consumption)

III. DEPLOYMENT OF APPLICATION ON CLOUD

This paper will satisfied with two security parameters such as authentication and separation of duties. Authentication is used to provide the identity of the particular user which requires creating the user id and password. In the application which is being created provides with two users which gets the accessibility one is admin and other is general user. Admin will be able to add., delete, modify and will be able to view the data whereas general user will be able to only view the data. In order to deploy the application on the cloud will have to follow the following steps:

- 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
- Create the WAR file of the Project.
- Upload a WAR file of project on the cloud.
- Deploy the WAR file on the cloud.
- Deploy the WAR file on the Environment.

While creating the cloud environment will have to go to the cloud link where we get the particular cloud will have to to create a WAR file and then will deploy the application on the cloud. Then connectivity with the cloud takes place in which the cloud is getting connected and the deployed application will then executed. After the connection is being established data of the application is saved on the cloud

IV. SECURITY ISSUES

A. Security issues in Cloud Computing:

There are many security issues in cloud computing that are faced much at the time of Encryption and data transmission major security issues are faced by cloud providers to ensure authentication, Integrity, Availability etc some of the issues are discussed below:

1) Intrusion Detection and Prevention: Data that is being entered and going out of the Network has to Know.

2) Separation of Duties: As complexity increases in the system miconfiguration takes place, because of insufficient Communication between the expertise.

3) Encryption: Original message is encrypted in such a way that third party will not able to read or hack the data[3] 4) Configuration and change control : These are the important parameters mostly found in small organizations. It needs to be maintained at virtual and physical world.

5) Authentication: Authentication is accepting proof of identity given by a credible person who has evidence on the said identity. Authentication requires while sending and receiving the message from one cloud to another. The concept of Digital Signature is used for getting the confirmation to check weather the message is send by original sender.

6) Physical Security: Provides security during the transmission of data and keeps the virtual system as well as cloud management host safe[1]

7) Location of Data: Different Organizations are their having their different requirements and control Placed on access. The level of security required by the customers to fulfill their needs is provided by the Cloud Providers

8) Service Level agreement (SLA): SLA serves as a sell service between cloud provider and the customer.

9) Access to Data: Anyone using cloud need to look at who is managing their data and what type of Controls is applies to these individuals [2].

10) Data Classification: This parameter is concerned with the type of Encryption mechanism , and Classification of Data

B. Cloud Characteristic:

1) Easy Use : Most Cloud Providers offers internet based interfaces . So Cloud services are being easily used by every user.

2) Business Model **:** Cloud is a business Model which is used to provide the services and the resource[8].

3) On Demand Service : Cloud is a service pool that will get the services continuously whenever we need by paying the amount that we want.

4) Ubiquitous Network Access : Assistants Cloud provides the services everywhere through the devices such as Mobile Phones, Laptops and Personal Digital.

C. Attributess in Cloud Computing :

1) Pay as U Used : Users have to pay for only the Resources they used.

2) Self Provisioning of Resources: Users have to pay only for the Resources they want.

3) Shared Resources : Cloud Computing provides the ability to scale to tens of thousands of systems as well as ability to massively scale storage space and Bandwidth .

V. ENCRYPTION ALGORITHM

There are various Encryption Algorithms such as DES, AES, 3DES, IDEA, Blowfish, RSA, ECC etc. For each Algorithm there are two key aspects used one is Algorithm type which defines size of Plaintext which is being encrypted per step and algorithm mode is the combination of Block Cipher and series of basic Algorithms.

A. Types of Encryption Algorithms:

1) DES: It encrypts data in block size of 64 bits each. It is a secret key cryptography which is of 56 bits long and same key is used for Encryption ad Decryption.

2) 3DES: This is an enhanced version of DES. In 3DES three times iteration is applied to increase average time and the Encryption level and it is of 56 bit.

3) Blowfish: The key length is ranging from 32 bits to 448 bits It uses block cipher of 64 bit block. Blowfish encrypts 64 bit blocks with variable length. For execution it requires less than 5kb of Memory.

4) RSA Algorithm: This is public key Encryption algorithm developed by Ron, Rivest Adi Shamir and Adelemann in 1977. It uses the same key for Encryption and Decryption and uses the prime number to generate the public and private key based multiplication of large numbers. In this Algorithm Encryption key should be known to the sender and Decryption key is known to the Receiver.

5) ECC: ECC was developed by certicom a mobile e-business security provider. Elliptical Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve Theory that can be used to create more efficient and smaller Cryptographic keys. ECC helps to establish equivalent security with lower computing power and battery resource usage. ECC is based on properties of particular type of Equation created from mathematical group. There is a set which is large but finite. There is a Group Operator is typically denoted by the symbol '+'. Every user has a public and private key. Public key is used for Encryption/digital Signature verification. Private key is used for Decryption/ Digital Signature Generation [6]. We have studied number of different techniques used for fulfillment of Data Encryption purpose. There are some Comparisons generated on different important features

A. Security issues in Cloud Computing:

There are many Security Issues in cloud computing that are faced much at the time of Encryption and data transmission Major Security issues are by cloud providers to ensure authentication ,Integrity etc some of the Issues are discussed below:

- Intrusion Detection and Prevention: Data that is being entered and going out of the Network has to Know.
- Separation of Duties: As complexity increases in the system miconfiguration takes place ,because of insufficient Communication between the expertises.
- Encryption: Original message is encrypted in such a way that third party will not able to read or hack the data [3]
- Configuration and change control: These are the important parameters mostly found in small organizations. It needs to be maintained at virtual and physical world.
- Location of Data: Different Organizations are their having their different requirements and control Placed on access. The level of security required by the customers to fulfil their needs is provided by the Cloud Providers**.**
- Service Level agreement (SLA): SLA serves as a sell service between cloud provider and the customer.
- Access to Data: Anyone using cloud need to look at who is managing their data and what type of Controls is applies to these individuals [2].

V. DATA PROTECTION IN CLOUD

Different types of clouds are present in order to store the data such as private cloud, public cloud, community cloud etc. Depending on the type of Cloud to be used the cloud provider will decide about the Infrastructure, Security and Operating System. There are various security Algorithms that are present which will protect the data in Cloud from the Attackers by encrypting the data before the Actual Transmission. The Information which is being transmitted in the network from one Cloud to another can be hacked by the third party which leads to loss of Security in order to, maintain the Security will have one best solution i.e. Cryptography which is used for protecting the Data. There are two methods of Cryptography:

A. Secret key Cryptography: A Key which uses for both Encryption and Decryption is called as secret key cryptography. IDEAS, DES, 3DES, AES, Blowfish are the Secret Key Cryptography Algorithms.

B. Public key Cryptography: Different keys are used for Encryption and Decryption then this key is called Public key Cryptography. RSA, Digital

Signature and Message Digest are the Public key Cryptography Algorithms.

VI. EXISTING TECHNOLOGY

RSA Algorithm is a public key encryption Algorithm which is widely used to encrypt the message as well as Digital Signature. No exchange of Secret keys will takes place in RSA Algorithm. A can select the encrypted message to B without exchanging the secret key. A uses the public key of B to encrypt the message and B will decrypt the message by using the private key. In RSA Algorithm user A picks up two prime umbers say p and q by using these numbers computation will takes place which results in their product as n=p*q. Now A‘s public key is the pair of integers {n,e} and
private key is d.
Following are the steps which takes place in RSA Algorithm for the generation of private and public key.
Choose large prime number p & q such that p~=q
Compute n=p*q
Compute $(p,q)=(p-1)*(q-1)
Choose the public key e such that
gcd ($(n) ,e)=1 ;1<e<$(n)
Select the private key d such that d*e(mod$(n)=1)
In RSA Algorithm Encryption and Decryption are performed by using the formulae as follows:
Encryption
Calculate Cipher text C from Plaintext message M such that
C=M^ e mod n
Decryption
M=C^ d mod n=M ^ ed mod n
RSA Algorithm will have the larger key size than the ECC Algorithm but even though they both will provide the same level of Security and also ECC will have better performance.

VII. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve Cryptography is one of the most secure and efficient Algorithm. This Algorithm is used for key exchange for sharing the public key certificates with end users. ECC is a public key cryptography Algorithm in which every participant will have pair of keys such as private key and
public key. Public key is used for Encryption/Signature verification and Private Key is used for decryption/Signature generation. Elliptic Curves are always cubic and group operator is one of the most important operators for ECC. Group Operator is typically denoted by the symbol
_+‘ even when the operation itself has nothing whatsoever to do with the ordinary arithmetic addition. An Elliptic curve standard form is given by:

$$y2 = x3 + ax + b$$

for some fixed values for the parameters a and b.
This equation is also referred to as Weiestrass Equation. The security of ECC Algorithm depends on its ability to compute a new point on the curve given the product points and Encrypt this point as information to be exchanged between the end users. Field is also an important part for the implementing an ECC Algorithm. An elliptic curve over a field K is a non singular cubic curve in two variables f(x,y)=0 with a rational point.

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 Discriminant must not become zero
3) It is not safe to use singular curves for
4) Elliptic Curve in their standard form will be Symmetric

VIII. PROPOSED PROCEDURE FOR DATA SECURITY IN CLOUD

Let us assume we have two Organizations say A and B in which A wants to send the Data to Cloud B and the data which is being transferred should be authenticated. Here the data is being encrypted using ECC will send from A to B. Suppose B wants a document from A’s Cloud then B used to send the request to cloud A. A will select the document and then by applying the hash function a Message Digest is created. Message Digest will gets signed with A’s private key which is called Digital Signature. The Encrypted Cipher text will send to B. B will decrypt the message with his private key and verify the signature using A’s public key.

IX. PROPOSED SYSTEM: ECC ALGORITHM

For the implementation of ECC Algorithm we consider mainly three Security parameters such as Authentication, Separation of Duties and Encryption for Secure data transmission from one cloud to other clouds that requires Authenticated data with Elliptic Curve Cryptography. In order to satisfy the above three security parameters will have to satisfy the following steps.

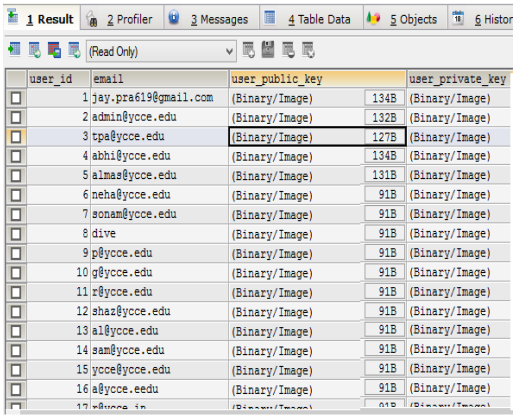
A. Key Agreement

Both clouds i.e. Cloud A and Cloud B will agree for the data which is being transmitted
1) The Elliptic Curve Equation
- Values of a and b
- Prime, p

2) By using the group operator Elliptic group is being computed from the equation of Elliptic Curve
3) Base Point is taken from the Elliptic Group.
The Agreement between the two parties will takes place only when both the keys are same.
1) A will select an integer XA = k1as his/her private key. The public key for A will be YA = XA × P, that is, a k1-fold application of the group operator to the point P, implying that while 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. The two parties exchange their public keys.
3) Subsequently, 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 = KB.
This proves the Agreement for exchanging the Data between two parties and the generation of public and private key.

B. Key Generation

Key generation is an important part where an Algorithm generates both the public key and private key. Here Sender A will encrypt the message with B's Public key and B will decrypt its private key.



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)

Fig 3:Key Generation

C. Encryption

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 travelled between the two parties and in between the way only the data is being encrypted. For the Encryption some nano seconds will be required to encrypt the data.
1) A takes a plaintext message M and encode it on point P from Elliptic Group by applying Group Operator '+'.
2) The Ciphertext is Pair of Points
C=[KB ,(P+KPB)]
3) Send Ciphertext to Cloud B

D. Decryption

In order to get the Original Message B will decrypt the message m by using his private key.

X. RESULTS

A. User Login

This is the Login Page of the Application where the user has to enter his User ID and Password. The user have to enter an accurate user Id and Password If the user is new then he will has to follow the Registration process After registration his all details will be Stored in the Database .New user will be able to logged in only after the Verification. If the User is Authenticated then only he will be allowed to enter in the System.

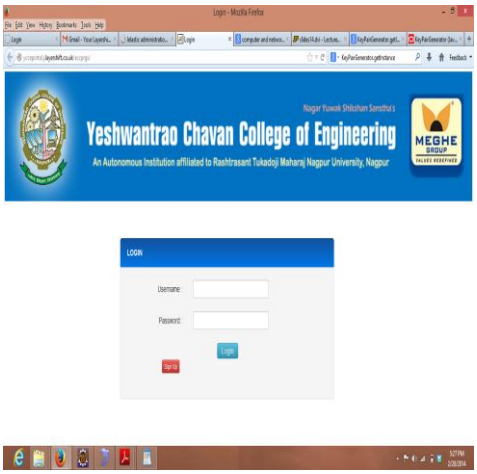


Fig.4: User Login

B. Digital Signature Generation

Digital Signature is used to maintain the Integrity. The data is being encrypted by using the digital signature which uses the hash Algorithm called as SHA 1.

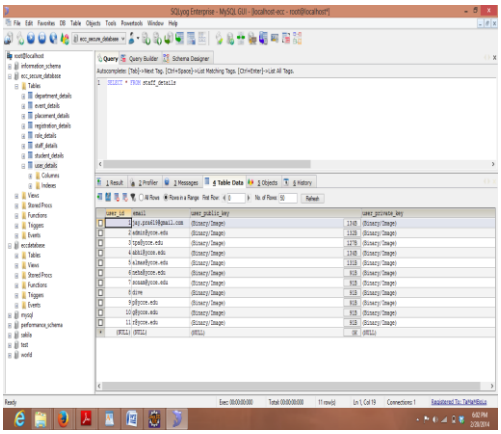


Fig 5:Digital Signature Generation

Digital Signature which is being generated will gets verified if third person will used to modify the data then we will came to know about the modification with the help of messages violated and verified.

Fig 6: Digital Signature Verification

C. Key Generation

It generates a key pair. Additionally, it displays on the screen the content of the public and private keys The key generation time was not the same even though the key length is same. Smaller key size will takes the less time for generation of key.

D. Key Agreement

When both i.e. the Sender and the Receiver will agree at a particular point for the transfer of data then only the data will gets transmitted.

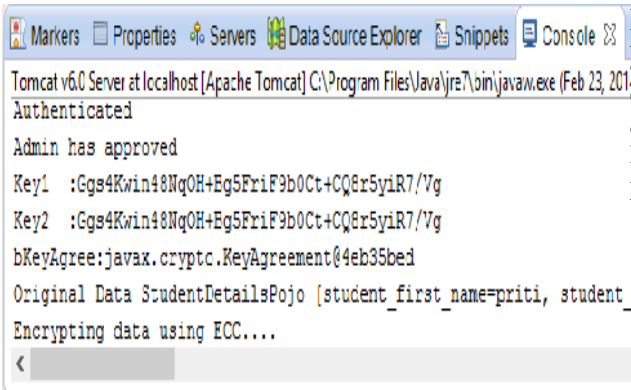


Fig 7:Key Agreement

E. Encryption and Decryption

After the Agreement Sender will sends the encrypted data to the Receiver and the encryption will takes place during the transmission of data so that the data which is send by the sender will as it is transmitted to the receiver i.e. receiver will receive the original data.

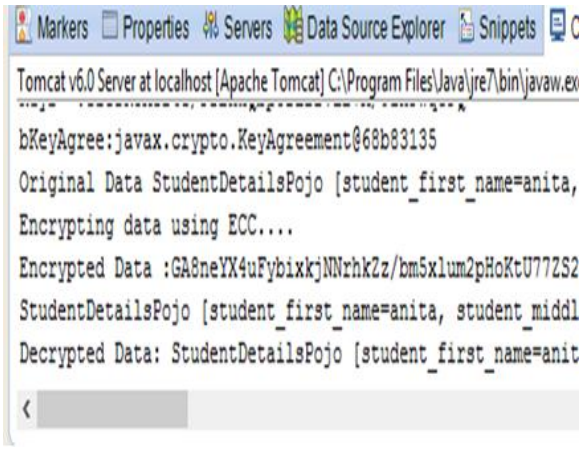


FIG 8: ENCRYPTION AND DECRYPTION

The Execution time for the Encryption of different Algorithms is compared. The speed of ECC Algorithm is twice times to the speed of DES and RSA Algorithm

XI. CONCLUSION

Now a day‘s Cloud Computing facing security Challenges. User put their data in the cloud and data is being transferred from one Cloud to another and users are concerned about the security. We concern higher security of Data and therefore we proposed an Encryption Algorithm i.e. ECC which takes least time to encrypt the Data than others and will ensures about the faster retrieval of Data. Security related parameters such as Encryption, Authentication and Access Control, Separation of Duties for the security has been satisfied in this Algorithm in order to achieve the Security. The presented simulation results showed that ECC has a better performance and more secure than other Encryption Algorithms. Future work is to newly propose a more secured system in which if the users access data without permission 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] 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

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

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

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

[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 IEEE

[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"