IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 72-77
www.iosrjournals.org

Deployment of Application and Review of Different Security Mechanism for Cloud

Neha Puri[1], Prof.R.C.Dharmik[2]

[1]*(Student, Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur India)*
[2]*(Professor, Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur India))*

***ABSTRACT** - Day-by-Day the cloud computing is been used widely in various areas because of its ability to reduce the costs associated with computing along with by increasing the scalability and flexibility for computing services. Cloud computing is a dynamic internet based computing where different services are provided to the user anywhere anytime when demanded. Because of the open environment of the cloud the biggest issue in the cloud computing is security. This paper will explore on efficient way of deployment of the application on the cloud and the review of the different security mechanism available for the cloud with their limitations and the drawbacks along with the some improvement factors in the available security mechanisms. Paper also focused on the literature on the new proposed technique for providing the advance security to the cloud which based on the encryption technique which will provide the very high security to the cloud*

***Keywords** - Cloud Computing, Encryption, Decryption, Cloud Security, Encryption Algorithms*

I. INTRODUCTION

Cloud computing is the novel style of computing where continous delivery of the resources in the form of services are taken place. It provides different level of Abstraction and Services to the Cloud users. There are the huge Opportunities that Cloud Computing offers for IT Industry. Cloud Computing is one of the best and fastest growing technology. Now a days Cloud Computing is in great demand in various field such as Scientific, Business, Medical etc. Also cloud is used very widely for college purpose as well to store the college data on the cloud.

A Cloud is a virtual space available to deploy the applications, whereas Cloud Computing is a general term for anything that involves delivering hosted services over the Internet .The main goal of Cloud Computing concept is to protect the data which comes under the property of Users [4]. At its simplest, it is delivering the resources and capabilities of information technology dynamically as a service. There are three services of cloud they are SaaS, PaaS, and IaaS

1.1 Cloud Services:

1.1.1 Software as a Service 0(SaaS): This services are Applications over Internet e.g. Google Docs.

1.1.2 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, are Testing, Deployment etc included in this service.

1.1.3 Infrastructure as a Service (IaaS): Computer Infrastructure is being offered by this services It delivers a platform virtualization Environment as a service rather than purchasing server, software, data centers

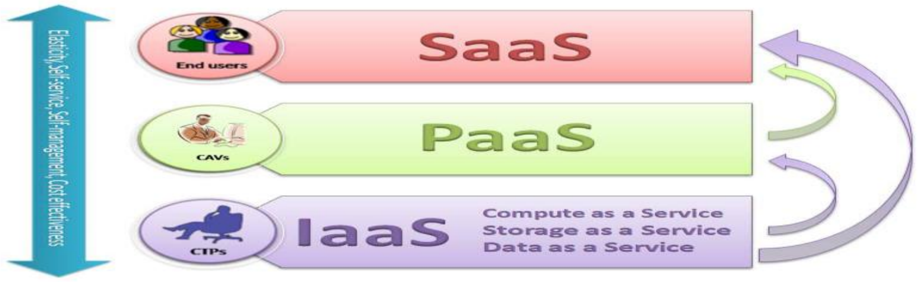

Fig1: Services in Cloud

1.2 Deployment Cloud Models:

1.2.1 Public cloud: The cloud infrastructure is made available to all people in other words we can say that ever one will be able to make use of this type of Cloud in order to store large amount of data

1.2.2 Private cloud: The cloud infrastructure is operated for an organization in order to store the private data. The main advantage of this type of cloud is security, compliance and QoS.

1.2.3 Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.

1.2.4 Hybrid cloud: The cloud infrastructure is a combination of public and private cloud .This is one the best option when someone will not able to or don't want to invest much in Infrastructure and on the want the security by using private cloud.

II. OVERVIEW OF SECURITY MECHANISM IN CLOUD

2.1 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:

2.1.1 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 wheather the message is send by original sender.

2.1.2 Intrusion Detection and Prevention: Data that is being entered and going out of the Network has to Know. Intrusion Prevention system could examine for Virtual Traffic Network.

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

2.1.4 Encryption: In this issue original message is encrypted in such a way that third party will not able to read or misuse it.

2.1.5 Configuration and change control: These are the important parameters mostly found in small organizations. It needs to be maintained at virtual and physical world.

2.1.6 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.

2.1.7 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].

2.1.8 Data Classification: This parameter is concerned with the type of Encryption mechanism, and Classification of Data.

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

2.2 Data Protection in Cloud:

Depending on the type of Cloud to be used the cloud provider will decide about the infrastructure, Network Security, Operating system, and Physical security of premises. To make the Data secure Different security Algorithms are present which will prevent the private data from attacks by encrypting the data before transmission. Various fields such as military, financial institutions, Government, Hospitals Business have their confidential data for e.g. enemy position in defense, geographical areas in Research. Most of the Information is being stored on the cloud due to which the transmission of data will takes place between the Clouds. The Information which is transmitted from network to other computers can be hacked by third party which leads to security loss, so in order to maintain the security will have one better solution i.e. The method of Cryptography which is an effective way of protecting sensitive data and information to be stored and transmitted across the network. There are two methods of Cryptography given below:

2.2.1 Secret key Cryptography: If same key is used for encryption and decryption then this key is called Secret key cryptography. In this method single key is used .Secret key Cryptography includes IDEA, DES, 3DES, AES, Blowfish Algorithm etc.

2.2.2 Public key Cryptography: If different keys are used for Encryption and Decryption then this key is Called Public key Cryptography. It includes RSA, Digital Signature and Message Digest Algorithm.

2.3 Comparison between Symmetric key Algorithms:

FEATURES	ECC	RSA	DES
KEY USED	DIFFERENT KEYS ARE USED FOR ENCRYPTION AND DECRYPTION.	DIFFERENT KEYS ARE USED FOR ENCRYPTION AND DECRYPTION	SAME KEY IS USED FOR ENCRYPTION AND DECRYPTION
PERFORMANCE	EFFICIENT	LOW	LOWER THAN ECC
SPEED	SPEED OF ENCRYPTION IS HIGH	LOWER SPEED OF ENCRYPTION	HIGH SPEED AS COMPARED TO RSA

CONFIDENTIALITY	HIGHLY CONFIDENTIAL	LOW	LOWER THAN ECC BUT MORE THAN RSA
THROUGHPUT	HIGH	LOW	VERY HIGH
AVALANCHE EFFECT	NO MORE EFFECTED	MORE EFFECTED	NO MORE EFFECTED

III. RELATED WORK

Cloud computing offers a utility model for IT, enabling users to access applications, middleware and hardware via the Internet as opposed to owning it themselves. 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. Reliability, availability and security are the three greatest concerns for moving on to the cloud. Businesses are running all kinds of applications in the cloud, like customer relationship management (CRM), HR, accounting, and much more. Some of the world’s largest companies moved their applications to the cloud with salesforce.com after rigorously testing the security and reliability of infrastructure [6].Cloud is a platform where data owner remotely store their data in cloud. The main goal of Cloud computing concept is to secure and protect the data which comes under the property of users [4]. Security is one of the serious issue in cloud computing. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. In order to achieve the security at highest level will have various Encryption Algorithms [2] such as Blowfish, RSA,AES etc. In this paper Authors had discussed various methods of Block Cipher Algorithms for providing solutions to cloud security. Amongst all the Encryption Algorithms ECC is one of the best Algorithm. In[3] ECC Algorithm is given In this paper Author has given various security parameter from which they considered only two parameters such as Authentication and Encryption or secure data transmission from one cloud to another that requires secure and Authenticated data with Elliptic curve Cryptography i.e. ECC. Encryption is a process of converting information in hidden form. In [1] comparison between DES and RSA Algorithm depending upon Execution time of decryption of different data packet size is given.

With shared infrastructure resources, organizations should be concerned about the service provider's authentication systems that grant access to data. The data is been encrypted using cryptographic keys to provide data confidentiality. Authenticating the users entering the network can also be done to secure the data [9].In [5] the authors consider a proposed Data Security model for which implemented a software which compares between eight modern encryption Algorithms to ensure Data Security. Depending on the NIST Statistical test they are going to compare the results and consider the fastest encryption speed Algorithm as the bestest one.
In our work we had adopted to create the cloud Environment by establishing the cloud connectivity and thereby maintain our data security by implementing an ECC Algorithm.

IV. PROPOSED WORK

Entire System deals with creating an application by collecting and analyzing the data of the department then that application has to be deployed on the cloud . There are two users one is simple user and another is Admin. We are trying to provide the authentication to Admin where as simple user will able to view only. In order to get the data on the cloud the user used to first login after getting the authorization he will be able to access the data . There are two Objectives that we want to achieve in this project one is Deployment and another is Security. Security is one of the serious issue in cloud computing is achieved by using the Symmetric key Algorithms. There are number of Security parameters that are discussed above the system is said to be completely secure if the algorithm will satisfy these parameters. Amongst all these Algorithms ECC (Elliptic curve Cryptography) is the only Algorithm which is used to satisfy most of the security parameters. During the transmission, data Attackers will hardly able to hack the data because by using this Algorithm the Security will increases to certain extent which makes our system more secure. We are trying to implement ECC Algorithm in our project which is public key cryptosystem [1] i.e. every user will have a Public key and private key. Here Encryption and Signature verification takes place with the help of Public key whereas Decryption and Signature generation will takes place with the help of Private key.

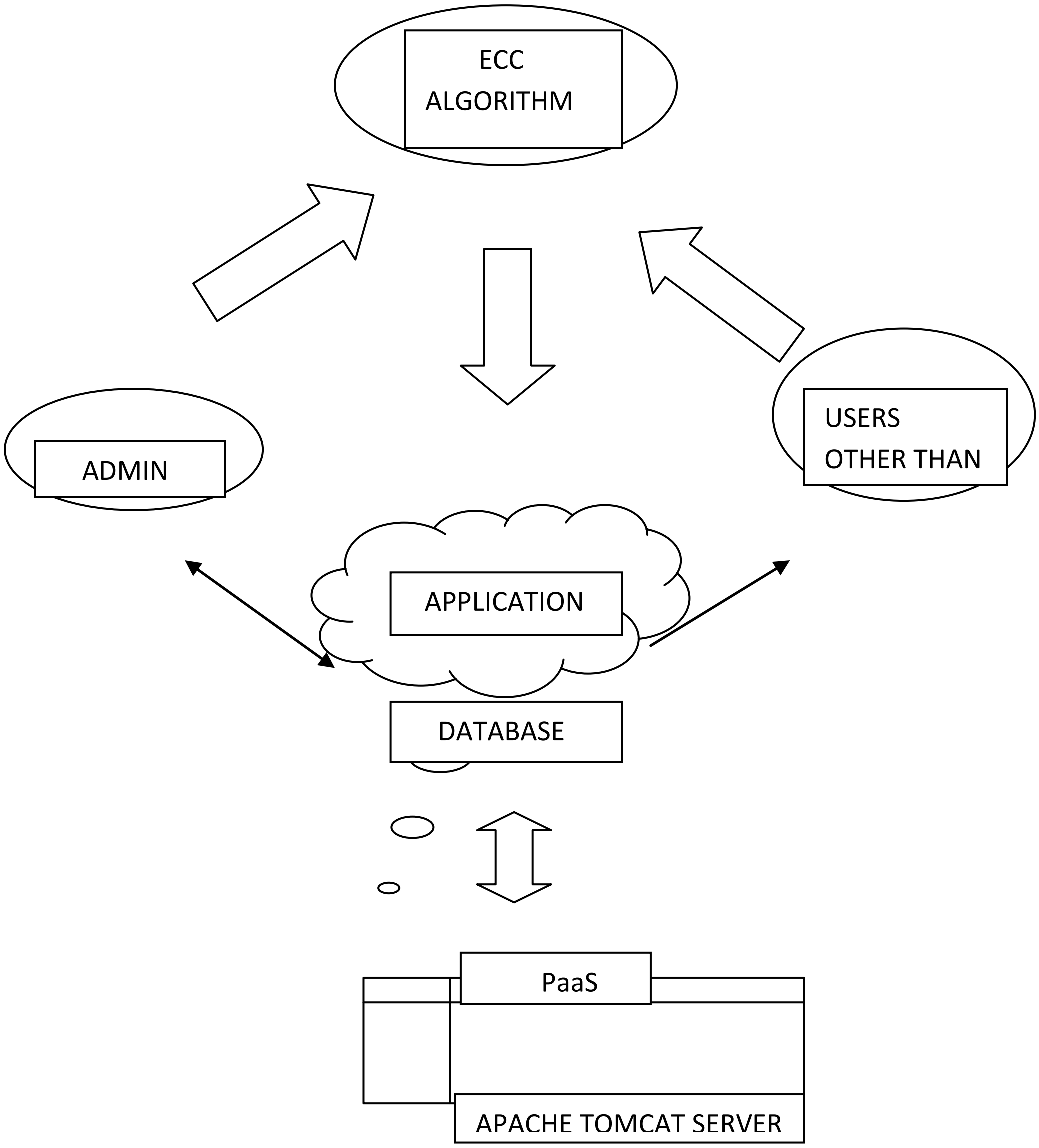

Fig 2: Architecture of the Proposed System

V. RESEARCH METHODOLOGY

We use here this methodology for getting the Results and the flow chart of our project is shown below:

In Cloud computing security plays the most important role. There are various services that are provided by the cloud provider to the users. In our project IaaS service is most important and we are using here the PaaS service for the Deployment of our Application which is our primary objective.. In order to maintain integrity as well as confidentiality of our Data we cannot able to trust on the service provider to handle the data because he himself can modify the original data [4]. Sometimes it may happen that if the Hacker is too smart he will hack the data and modify it and this modification will not identifiable by the cloud provider. In this case we are going to implement the encryption Algorithm i.e. ECC which will take care for the security of data which is being deployed on the cloud. We are going to implement here the three security issues of cloud computing which helps us to make our system more secure.

VI. CONCLUSION

Now a days Cloud Computing facing security Challenges. User put their data in the cloud and data is being transferred from one Cloud to another users are concerned about the security. In this paper, we concern higher security of Data and therefore we are proposing 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 is next to implemented in the Algorithm in order to achieve the Security. Thus our aim of deployment of application on the Cloud and maintaining its security is being satisfied.

REFERENCES

[1] Aman Kumar, Dr.suresh. Jakhar, and Sunil Makkar Comparative Analysis between DES and RSA Algorithms, *International Journal of Advanced Research in Computer Science and Software Engineering, volume 2.Issue 7 ,July 2012.*

[2] Leena Khanna, Prof.Anant Jaiswal, Cloud Computing: Security Issues and Description of Encryption Based Algorithms To Overcome Them. *International Journal of Advanced Research in Computer Science and Software Engineering, volume3,no 3,March 2013.//**

[3] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, 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*

[4] Ashish Bhagat, Ravi Kant Sahu, Using Third Party Auditor for Cloud Data Security: A Review, *International Journal of Advanced Research in Computer Science and Software Engineering ,volume3,no 3,March 2013*.

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

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

[7] N. Jenefa, J. Jayalakshmi ,A Cloud Storage System with Data Confidentiality and Data Forwarding, *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March-2013*

[8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, BhavaniThuraisingham" Security Issues for CloudComputing*"International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39*

[9] N. Jenefa, J. Jayalakshmi "A Cloud Storage System with Data Confidentiality and Data Forwarding" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March-2013

[10] *http://searchcloudcomputing.techtarget.com/resources/Data-security-in-the-cloud*