ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A REVIEW OF DIFFERENT ENCRYPTION ALGORITHM FOR CLOUD COMPUTING

Mr.Ajay Ramesh Karare*1 & Dr.Sachin Choudhari2

*1&2Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur (MS) India

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]

Security of data which is being stored and data in transmit may be a concern when storing sensitive data at a cloud storage provider

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)[4]

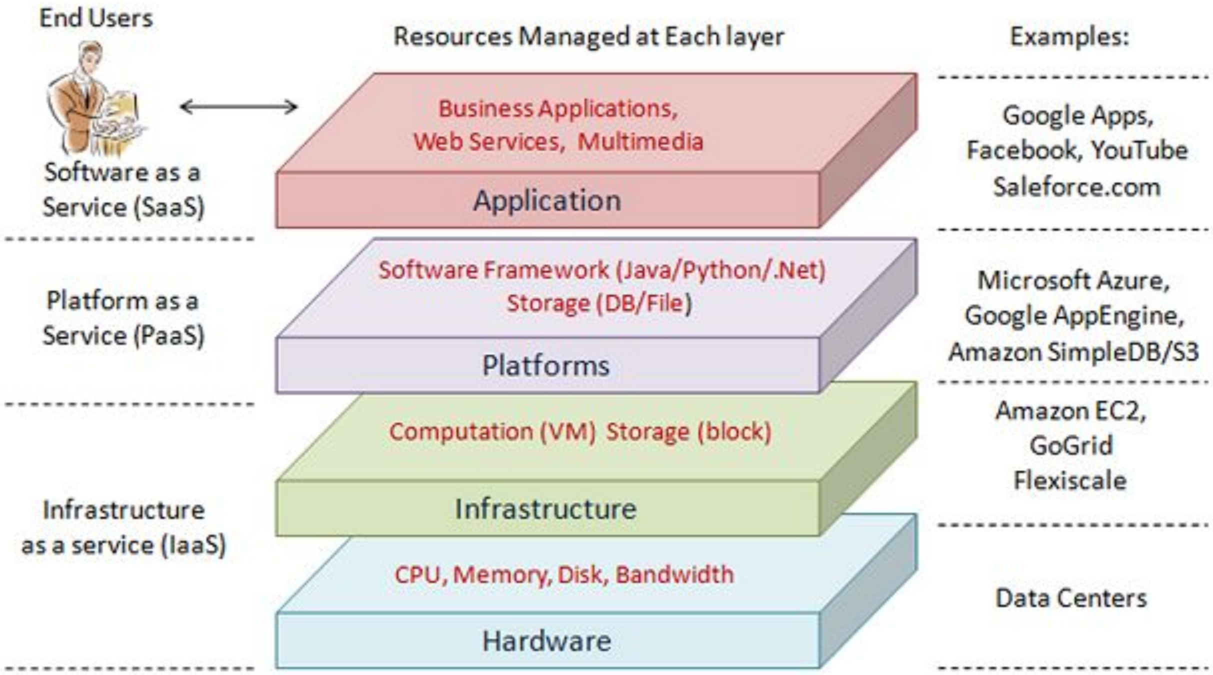

End Users
Resources Managed at Each layer
Examples:
Software as a Service (SaaS)
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Platform as a Service (PaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Fig.2. Service Model in Cloud Computing

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 select the cloudlets i.e. the amount of space on the Cloud. Will have

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

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:

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 expertise.

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.

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.

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

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

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].

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

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

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

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

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

Attributess in Cloud Computing :
Pay as U Used : Users have to pay for only the Resources they used.
Self Provisioning of Resources: Users have to pay only for the Resources they want.
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.

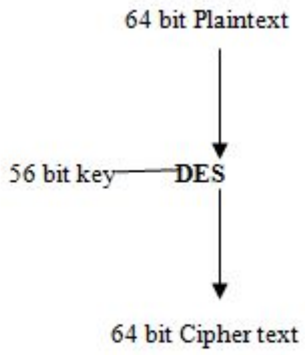


Fig.3. DES Block

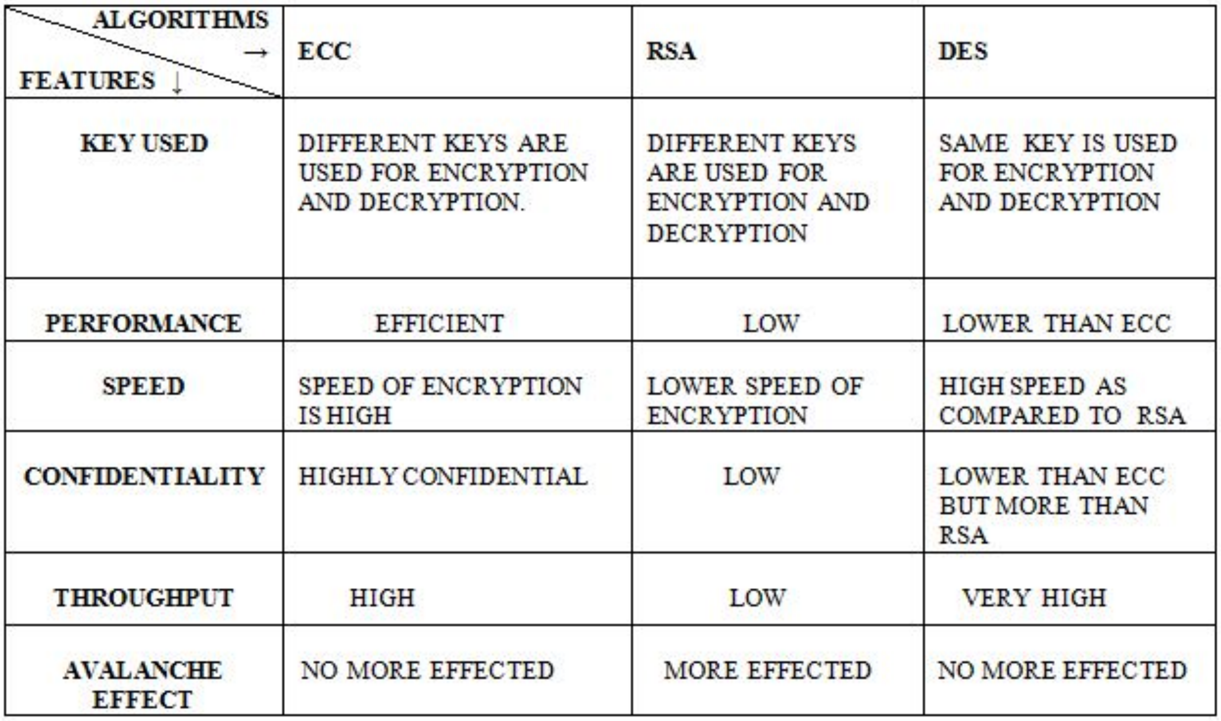
2) 3DES: This is an enhanced version of DES. In 3DES three times iteration is applied to increase average time and the Encryption level and it is of 56 bit.
3) Blowfish: The key length is ranging from 32 bits to 448 bits It uses block cipher of 64 bit block. Blowfish encrypts 64 bit blocks with variable 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.

TABLE I. Comparisions Between Different Encryption Algorithms



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

VI. 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 going to implement the encryption Algorithm i.e. ECC which deployment of our application which is our primary object ective.. 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 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.

TABLE II. Authors and Detail Description of their Papers

Sr.no	Title of Paper	Author	Description
1.	Deploying an Application on the Cloud	N. Ram Ganga charan, S. Tirupati Rao,Dr .P.V.S Srinivas	Storing the application on cloud ,concerns of cloud storage and application development platforms over the internet using cloud computing
2.	Enhanced Data Security Model for Cloud Computing	Eman M.Mohamed , Hatem S. Abdelkader, Sherif EI-Etriby	Different types of data in cloud computing and security of data on the cloud .
3.	Data Security and Privacy Protection Issues in Cloud Computing" 2012 International Conference on Computer Science and Electronics Engineering	Deyan Chen , Hong Zhao	Protection issues in order to secure the data on cloud
4.	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	N. Jenefa, J. Jayalakshmi	Confidentiality and forwarding of the data to the user is described.

VII. CONCLUSION

This paper tells the importance of protecting privacy in Cloud Computing .Thus by satisfying the various security parameters only the Authorized users will able to access the data in the Cloud. If the user accesses the data without permission he will be blocked immediately in order to increase the security of data which is required for deploying the Application on the cloud. Elliptic Curve Cryptography provides greater security and more efficient performance than other encryption like RSA. The future of ECC looks brighter RSA. The work is further extended by using ECC which is used for Digital Signature, Key exchanges as well and to provide Data integrity and Confidentiality

REFERENCES

[1] 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

[2] 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.

[3] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. of ACM workshop on Cloud Computing security (CCSW'09), 2009, pp. 43–54.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp:Multiple-replica provable data possession," in Proc. of ICDCS'08. IEEE Computer Society, 2008, pp. 411–420.

[5] 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

[6] 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-2013J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[7] *K. Chine, "Scientific Computing Environments in the age of virtualization," Proc. of IEEE International Workshop on Open-source software for scientific computation (OSSC 2009),2009*

[8] *P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory 2009*