International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 4 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

# Comparison among RSA, AES and DES

**Heena Arora[1], Jaishree Jain[2]**

*[1]Assistant Professor, Computer Science and Engineering, AIT Department, Chandigarh University, Mohali, Punjab*
*[2J] Assistant Professor, Computer Science and Engineering, AIT Department, Chandigarh University, Mohali, Punjab*

---

**Abstract –** *As we know securing the data is becoming a big issue now a day. Today is the era of technology, so there is big need to keep our data very secure. As numbers of users are increasing day by day the need to secure the data is become a big challenge now. First of all, we need to classify that data before securing it. Though classification we divided the data. In this paper we divided the data into two parts sensitive and non-sensitive. By the usage of KNN classifier classification is performed initially. Than by apply different security mechanisms and performed the comparison among these security algorithms. We apply RSA, AES and DES one by one to our datasets. We calculate at end encryption time. Securing the data is challenging task. If we want security than there is need to keep the data very secure. Through security we provide confidentiality to the users. The results obtained at end shown AES is strongest as compared to DES, RSA.*

***Key Words***: **Cloud Computing, Cloud Security, Classifier, AES, RSA, DES**

## 1. INTRODUCTION

For secure and save our data encryption is a good method. Cloud security refers to broad set of policies, technologies and controls deployed to protect data, associated applications and the infrastructure of cloud computing. Cloud Computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models and deployment models. Security concerns associated with cloud computing fall into two categories: Security issues faced by cloud providers and security issues faced by their customers.

Somani and Mundra (2010) proposed RSA algorithm issued to ensure the confidentiality aspect of security where as digital signatures were used to enhance more security by authenticating it through digital signatures. The approach used carryout encryption in 5 steps. In first step key is generated in second step digital signing is performed and in step 3 and step 4 encryption and decryption were carried out in last step signature verification is performed.[1]
Dubey and Shrivastava (2012) they provide at two-way security protocol which helps both the cloud and the normal user. They applied RSA and MD5 algorithm. When the cloud user uploads the data in the cloud environment, the data is uploaded in encrypted from using RSA algorithm and the cloud admin can decrypt using their own private key for updating the data in the cloud environment admin request the user for a secure key.
Cloud users ends a secure key with message digest tag for updating data if any outsiders perform a change in the key, the tag bit is also changed indicating key is not secure and correct.[2]

### 1.1 Methodology

#### A. DESIGN SIMULATION SCENARIO

Initially we design simulation environment with the help of Cloud Sim.

#### B. COLLECT DATASET

In this we collect employer data from an organization.

#### C. Apply Machine Learning Algorithms for classification the data

To get sensitive data KNN classifier is used.

**D. Apply Cryptographic Algorithm to Sensitive Data**

After finding the sensitive data is further transferred to RSA, AES and DES for data encryption.

**E. Analysis the Result**

At the end results has been analyzed and results obtained at end shown AES is strongest as compared to RSA, DES .

## 1.2 Problem Formulation

The data stored in cloud needs confidentiality, integrity and availability. Cloud computing is a new technology which is being used by lots of organization. It provides services and resources to its users. But to handle security risks in cloud is a challenging task. Cloud computing needs to address three main security issue confidentiality, integrity and availability. There is need to use some efficient methods to keep data secure. There should be used some security algorithms which provide encryption, authorization, confidentiality, integrity and availability. In this study various security issues at the level authentication and storage level in cloud computing. For securing the data it is very compulsory to divide the data into different categories, than after that according to these categories there is need to apply security mechanisms. For classify the data we use in this paper KNN classifier.
KNN is based on neighbor instances. Classification based on KNN Classifier used neighbor distances .This classifier used the technique based upon nearest neighbor. This classifier classifies the data into different categories like sensitive, non-sensitive. As according to need different security algorithms can be used. So this is the way through which we can keep our data secure in cloud. On sensitive data different algorithms have been used like DES, RSA, and AES.

## 2. Results and Discussions

A. Input Datasets(X)

| ID | CableOperatorId |
|---|---|
| Name | Cable Operator Name |
| Digitization Status | True: if Digital, False: if not Digital |
| City | Cable Operator City |
| District | Cable Operator District |
| State | Cable Operator State |
| Zipcode | Digitization Area Zipcode |
| Area | Cable Operator Area |
| Longitude | Longitude of Cable operator |
| Latitude | Latitude of Cable operator |
| Location | Location |

**Figure -1:** Input Datasets(X)

### B. Output Of Proposed Work

| Cloud ID | STATUS | Datacenter ID | Start time(ms) | Finish time(ms) |
|---|---|---|---|---|
| Normal dataset | 0_success | 2 | 0.2 | 160.2 |
| AES | 1_success | 3 | 0.2 | 1280.2 |
| RSA | 2_sucess | 3 | 0.2 | 2560.2 |
| DES | 3_success | 3 | 0.2 | 2433.2 |

**Table -1**: Output of Proposed Work

In figure 2 there is representation of How Cloud-Sim Works as shown below.

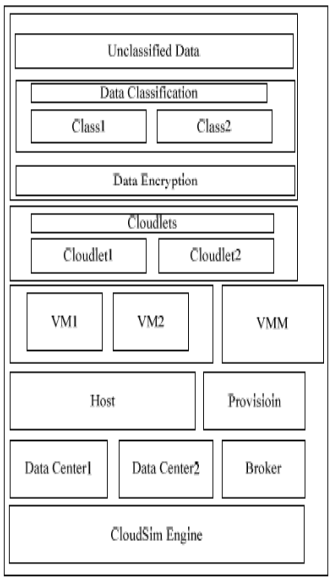


**Fig -2**: How Simulation Environment Work

## 3. CONCLUSIONS

The main aim of implementation of this project is to provide the security. In this paper we encrypted the data after applied KNN classifier than we apply different algorithms like RSA, AES and DES. For classify the data we classified into sensitive and non -sensitive parts. The data which is sensitive, on this data we applied different algorithms RSA, DES and AES and calculate the encryption time and performed comparison of different algorithms. At the end after comparing we find AES is strongest algorithm for security and fast as compared to RSA and DES. In future we will use SHA-256 or hashing algorithm to provide the security. and in future we also will use naïve Bayes classifiers. The results shown to us at end, clearly described that AES is fastest and provide more security as compared to RSA and DES.

## REFERENCES

[1] Dubey A.K., Namdev M., Shrivastava S., "Cloud- User security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", 6th IEEE International Conference on Software Engineering (CONSEG), vol.1, pp.1-8, Sept.2012.

[2] Diwan V., Malhotra S., Jain R., "Cloud security solutions: Comparison among various cryptographic algorithms", IJARCSSE, April 2014.

[3] D. Purushothamanand S. Abburu, "An approach for data storage security in cloud computing", IJCSI International journal of computer sciences issues, vol. 9, issue 2, March 2012.

[4] D. Chenand H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing",2012 Int. Conf. Comput.Sci.Electron.Eng.vol.1, no. 973, pp.647-651, 2012.

[5] Arcokiam L., Monikandan S., "Efficient cloud storage confidentiality to ensure data security", Int. Technol, Tomorrow, Today, ICCC1, vol.1, pp.1-5, 2014. Conf. Comput. Commun. Informatics Ushering.

[6] AlJaberi M. F., Zainal A., "Data Integrity and privacy modeling Cloud computing", pp.280-284, 2014.

[7] Rewagad P., Pawar Y., "Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing", International Conference on communication system and network technologies (CSNT), vol.1, pp.437-439, Apr. 2013

[8] Somani U., lakshani K., Mundra M., "Implementing digital signatures with RSA encryption algorithm to enhance the data security of cloud in cloud computing",1st IEEE international conference on parallel Distributed and grid computing (PDGC), vol. 1, pp.211-216, Oct. 2010.

[9] Yellamma P., Narasimhams C., Sreenivas V," Data security in cloud using RSA", 4th IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT), vol. 1, pp.1-6, Jul.2013.