IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 3 ISSUE : 11 Print / Issue Publication Date: 29-May-2019

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2019.v03i11.009

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 3, Issue 11, ISSN No. 2455-2143, Pages 42-46
Published Online March 2019 in IJEAST (http://www.ijeast.com)

MULTI-LEVEL SECURITY

Ashish Suri, Dhruv Pathak, Pratik Naik
Student, Department of CSE
Lokmanya Tilak College of Engineering,
Koparkhairane, Maharashtra, India

Archana Naware
Professor, Department of CSE
Lokmanya Tilak College of Engineering,
Koparkhairane, Maharashtra, India

Abstract- Cloud Computing is just like a large pool, in which various accessible and virtualized resources are available. These resources include hardware, development platforms and services. In Cloud Computing, it is possible to assemble very large, powerful systems; these systems may consist of many small and inexpensive commodity components. Cloud Computing is the emerging technology, that is used for providing various computing and storage services over the Internet. Information security is a critical issue in Cloud Computing environments. Clouds have no borders; hence the data can be physically located anywhere in any data centre across the network geographically distributed. In this paper, I work on the Cloud Computing security wherein I use the RSA algorithm to encrypt the data and image sequencing password for authentication.

Keywords-**Cloud Computing, Security, RSA, Image Sequencing.**

I. INTRODUCTION

Cloud is an internet based technology that uses the internet and central remote servers to support data and applications. The Cloud Computing permits many users to access the system without installation of personal files on any computer but with internet access. In Cloud Computing, websites and server based applications are executed on a specific system. The Cloud Computing flexibility is a function of the allocation of resources on authorized request. It generally incorporates infrastructure, platform, and software as services. These service providers rent data-center hardware and software to deliver storage and computing services through the Internet. Internet users can receive services from a cloud as if they were employing a super computer. The data can be stored on a cloud rather than storing it on their own devices which also makes ubiquitous data access possible. They can run their applications on much more powerful Cloud Computing platforms with software deployed in the cloud which mitigates the user burden of full software installation and continual upgrade on their local devices

Implementation Plan

Sender Panel:-

Sender Registration:-Sender fills registration form. Form having all personal information with their password sequence. Sender have to define a image sequence for the login procedure. Image Sequence will get store into the database. Sender will receive a mail which contains Sequence of images which he specify during Registration. Which will help to recover password anytime.

Sender Login:- When Sender try to login into the system, he have to enter a username for the verification. If that username present into the database then randomly place image grid will get display. Sender have to follow the sequential which he specified during registration. If the sequence match with the previously define sequence then sender login into the system or else he will get invalid username or password alert message.

Upload File:-Sender browse the file which he wants to share with receiver. Also he will specify the email id of the receiver.

Encryption Using RSA:-After uploading file application encrypt the file using RSA algorithm and store into the folder and database. No one will open the encrypted file because its encrypted using public key.

Cipher Text:-After Encryption using RSA algorithm Encrypted file is store into the secure folder. Mail Private Key Via Email:-Algorithm generated private key is share with receiver via mail. which will help to decrypt the file.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 3, Issue 11, ISSN No. 2455-2143, Pages 42-46
Published Online March 2019 in IJEAST (http://www.ijeast.com)

Receiver Panel:-

Receiver Registration:- Receiver fills registration form. Form having all personal information with their password sequence. Receiver have to define a image sequence for the login procedure. Image Sequence will get store into the database. Receiver will receive a mail which contains Sequence of images which he specify during Registration. Which will help to recover password anytime.

Receiver Login:- When Receiver try to login into the system, he have to enter a username for the verification. If that username present into the database then randomly place image grid will get display. Receiver has to follow the sequential which he specified during registration. If the sequence match with the previously define sequence then sender login into the system or else he will get invalid username or password alert message.

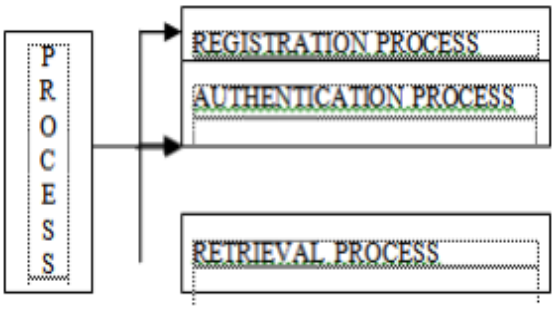
View File:-Receiver view the list of the files which are share by sender. Receiver can see file name, Share by person name, date time.

Enter Private Key for File Decryption:-once receiver click on download button, new window will get open. He have to enter the key which is receive via mail.

Download File:- if the key matches system automatically decrypt the file and download into the system. And receiver can now access the file effectively.

SYSTEM ARCHIECTURE

Proposed System Architecture



The processes involved in this project are shown in above diagram
The following explains the sequence of steps involved in image based password. At first user requested to sign up by entering the name, date of birth, phone number, mail id and then user is provided with 3 images and the user must click one point per image. The images may be predefined or users wish. These click points are encrypted and decrypted using RSA cryptographic algorithm, which brings better security to the system. For login the user must select the same click points. If the user fails to select the correct password for more than 3 times, the user account would be locked and the account would be unlocked by entering the random alphanumeric text that has been sent to the authorized person mail. This approach would bring security and authorization to the system.

A. Service Models Of Cloud Computing:

Once a cloud is developed, it can differ from its requirements. There are various models we use in Cloud Computing .These models are:

Cloud computer services

· *Software as a Service (SaaS)*

In the SaaS, the consumers purchase the ability to access and use an application or service that is hosted in the cloud.

· *Platform as a Service (PaaS)*

In the PaaS, the consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud.

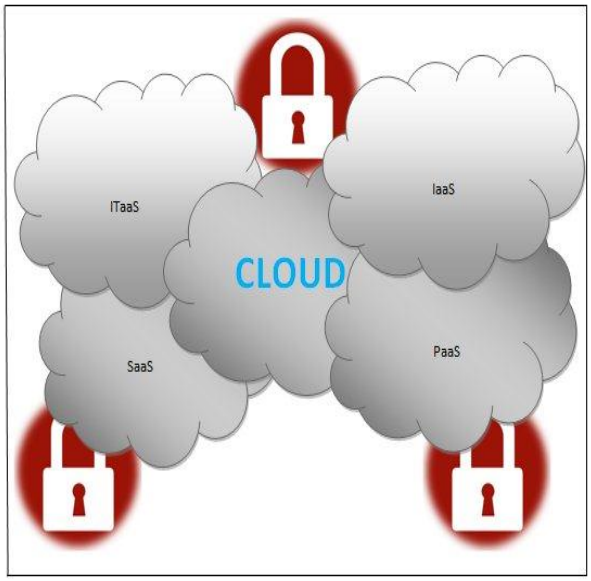
· *Infrastructure as a Service (IaaS)*

Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity. Communications as a Service model is used to describe hosted IP telephony services. Physical infrastructure is abstracted to provide computing, storage, and networking as a service, avoiding the expense and need for dedicated systems.

B. Deployment Models of Cloud Computing:

Deploying Cloud Computing depends on various requirements; hence it is different from other technology. As far as deploying a cloud is concerned, four deployment models can be used wherein each model has its specific characteristics

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 3, Issue 11, ISSN No. 2455-2143, Pages 42-46
Published Online March 2019 in IJEAST (http://www.ijeast.com)



· *Private Cloud*

The private cloud is used for the personal work, as the private cloud can be maintained and operated by a specific organization. The operation may be in house or with a third party on the premises.

· *Community Cloud*

This cloud is shared among the various organizations having the same or similar interests and requirements. This may help to limit the capital expenditure costs for its establishment as the costs are shared among the organizations.

· *Public Cloud*

The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables the consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements.

· *Hybrid Cloud:*

The cloud infrastructure may consist of number of clouds of various types, but the clouds have the ability through their interfaces to allow data or applications to be moved from one cloud to another. This can be a combination of private and public clouds.

II. PURPOSED WORK

Currently, Information security plays one of the major critical issues in Cloud Computing environments. Clouds have no borders and the data can be physically located anywhere in any data centre across the network. The network is geographically distributed, So the nature of Cloud Computing raises serious issues regarding user authentication, information integrity and confidentiality. With the cloud model, you lose control over physical security.

In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you do not have any knowledge or control of where the resources run. Storage services provided by one cloud vendor may be incompatible with another vendor services. Data integrity is the assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions. The cloud service provider for cloud makes sure that the customer does not face any problems such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud so I think that an effective user authentication system should be available which provides access only to the authorized people.

III. METHODOLOGY:

There are basic two types of attacks:

· Active attacks

·Passive attacks

In passive attacks, the data confidentiality breaks since the third parties have access to your data but cannot do any modification in the data[1]. In active attacks, the data integrity breaks since the data can be modified by the third party and it can be sent back to the user.
To solve the problem of security in Cloud Computing, we are going to use two ways of security process in Cloud Computing. Here I use an image sequence based password which provides security for user authentication attacks at user end and I use RSA Algorithm for secure encryption of data over the cloud.
There are various other security services used in Cloud Computing:

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 3, Issue 11, ISSN No. 2455-2143, Pages 42-46
Published Online March 2019 in IJEAST (http://www.ijeast.com)

· *Authentication* - Assures that the communicating entity is the one claimed

· *Access Control* - Prevention of the unauthorized use of resources

·*Data Confidentiality* - Protection of data from unauthorized disclosure

·*Data Integrity* - Assures that data received is, as sent by an authorized entity

Non-Repudiation - Protection against denial by one of the parties during communication

IV. IMPLEMENTATION

In this Paper, I'm going to use the image sequencing password with RSA to enhance the security of Cloud Computing.

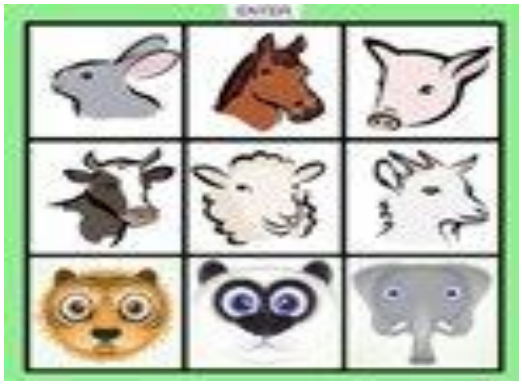


Image Sequencing fig 2

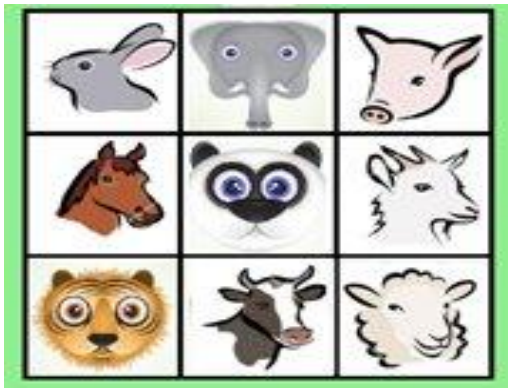


fig 3

Suppose in this we use the horse-cow- goat-panda, and fix this as the password so the sequence number will be 2468. So when we enter the sequence number, we get access to enter our cloud. Apparently this sequence will always be changed whenever the system is logged on so that the password sequence is same but the position changes so that the numbers are changed.

Here in fig 3, the position of the animals are shuffled hence our password is also changed. Now our password becomes 4865 according to the position of horse-cow-goat-panda. So this process consecutively happens which makes the password unbreakable. Since there is no password or algorithm which is so secure; I use RSA encryption to protect the data further more.

We use the RSA algorithm as:

1. Choose two large prime numbers P and Q
2. Calculate N = P x Q
3. Select the public key (i.e., Encryption Key) E such that it is not a factor of (P-1) and (Q- 1)
4. Select the Private key (i.e., Decryption Key) D such that the following equation is true;
5. (D X E) mod (P-1) X (Q-1) = 1
6. For encryption, Calculate the cipher text CT from the plain text PT as follows:
7. CT = PT^E mod N
8. Send CT as the cipher text to the receiver
9. For Decryption, Calculate the plain Text PT from the cipher text CT as follows: 10. PT = CT^D mod N.

V. CONCLUSION

Cloud is totally a distributed environment with heterogeneous networks geographically, so a security system like this will absolutely make a mark in providing better solution to the major issue called security and which further more gives an efficient performance in terms of Authenticity.

VI. REFERENCES

[1] Stallings, William, "Public Key Encryption and RSA," in Cryptography and Network Security, 5th ed. Published by Pearson Education, Inc, Copyright © 2011, pp. 293-314.

[2] John W. Rittinghouse, James F. Ransome, "Web Services Delivered from the Cloud," in Cloud Computing Implementation, Management, and Security, *CRC Press Taylor & Francis Group 6000*

Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, Copyright © 2010 by Taylor and Francis Group, LLC, pp. 48-95.

[3] Somani, Lakhani. K, Mundra. M, "Implementing digital
signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing, "in *Proc. Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference, Solan, 28-30 Oct 2010, pp.211- 216.*

[4] AlZain, Soh, Pardede, "Using Multi-clouds to Ensure Security in Cloud Computing, "in *Proc. Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference, Sydney, 12-14 Dec. 2011, pp. 784 - 791.*

[5] Wentao Liu, Dept. of Comput. & Inf. Eng., Wuhan Polytech. Univ., Wuhan, China "Research on cloud computing security problem and strategy, "in *Proc. Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference, Yichang, 21-23 April 2012, pp. 1216 - 1219.*

[7] Cong Wang et.al, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, This paper was presented as part of the main Technical Program at IEEE INFOCOM 2010.

[8] Parsi Kalpana, Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[9] Neha Tirthani Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography

[10] Rashmi Nigoti,Manoj Jhuria, Dr.Shailendra Singh, A Survey of Cryptographic Algorithms IASIR Computing , nternational Association of Scientific Innovation and Research (IASIR)

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143