IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

Multi-Level Security in Cloud Computing Technology

Tejas Kadam[1], Anas Shaikh[2], Hariom Gurjar[3], Rahul Patil[4]

Student, Computer Technology, Bharati Vidyapeeth, Navi Mumbai, India[1,2,3]

Lecturer, Computer Technology, Bharati Vidyapeeth, Navi Mumbai, India[4]

Abstract: Cloud computing is being projected by several major IT companies such as IBM, Google, Yahoo, Amazon and others as fifth utility where clients will have access for processing those application and or software projects which need very high speed for compute intensive and huge data capacity for scientific, engineering research problems and also e-business and data content network applications. this direct access service management based on virtualization of hardware, software and very high bandwidth internet communication. The paper reviews these developments for cloud computing and examines the claims being made by the major cloud computing provider companies and a future prospect of the ISP based services. It also high lights the IT industry's concerns for cloud computing

Keywords: Cloud Computing, Security, RSA, Image Sequencing

I. INTRODUCTION

Authentication is the process where the system checks whether the user is authorized or not. Text-based password is the mostly used by authentication system. A text password is nothing but a bunch of characters with strong encryption and decryption algorithm. But nowadays user can’t remember strong password easily they create text passwords with pet names, phone number, etc. which is easy to remember or guess by the human brain. But password created must be easy to remember but hard to guess. Our human brain is better at remembering images than text. Image passwords are meant for reducing the memory saddle on users. Image passwords may offer better security than text-based passwords because most of the people, in an attempt to memorize text-based passwords, use simple words. Pass faces is a graphical password scheme where user needs to select the images from the large number and to login the user must identify one of the preselected images amongst several images. Draw - A - Secret (DAS) is a graphical password scheme where user is requested to draw a picture using mouse or stylus. The coordinates of the grids i,e.,(X,Y) that had been occupied by certain picture are stored . To login the user is requested to re-draw the same image. If the user draws the same image in the same grids, then the user is authenticated. An alternative scheme is based on creating story using images . This would make users to select their images in the correct order. Users were encouraged for creating a story as a memory assist. In this project, we propose an image-based password authentication. A password consists of one click per image for a multiple image. The image may be predefined or user defined. Image based password offers both improved usability and security.

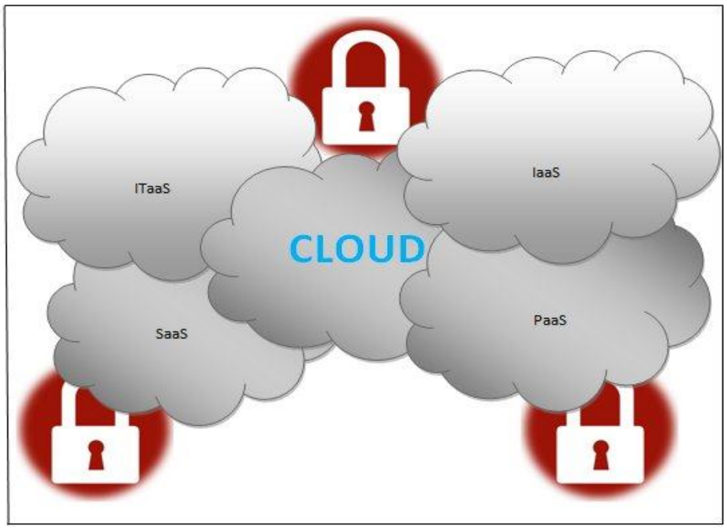

Fig 1: Cloud Computer Services

DOI 10.17148/IJARCCE.2020.9220

 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. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed.
 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.

II. LITERATURE SURVEY

Cloud Computing has been visualized as the heir framework of IT consortium. Cloud Computing moves the application software and databases to the data centers. This in turn imposes many new security challenges which are not clear yet. This paper gives a detailed introduction of cloud computing its types and security issues and approaches to secure the data into cloud system. Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Cloud computing is useful to think of a cloud as a collection of hardware and software that runs in a data centre and enables the cloud computing model and data security. These can be analyzed by reviewing some existing researches.

Technical Information

Existing System: Pass-points is a method where user needs to select five points on the image for register. For authentication user needs to select five click points in the same order. In cued click points, user can select one click point for one image up to n levels. In login phase user should follow the order and select the click point.

Proposed System: To solve the problem of security in cloud computing, we are going to use two-way security on cloud computing. Here image sequence base password provides security from authentication attacks at user end. RSA Algorithm use for secure encryption of data over our cloud

There is various security services used in the cloud computing as:

- Authentication - assurance that the communicating user is authorized claimed
- Access Control - prevent the unauthorized use of a resource
- Data Confidentiality –protect the data from unauthorized activity
- Data Integrity - assurance that data received is sent by an authorized entity
- Non-Repudiation - protection against one of the parties in a communication

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 . 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 security services used in Cloud Computing:
- 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 getting to use the image sequencing password with RSA to reinforce the safety of Cloud Computing.

Suppose during this we use the horse, cow, goat, panda, and fix this because the password therefore the sequence number are going to 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.

DOI 10.17148/IJARCCE.2020.9220

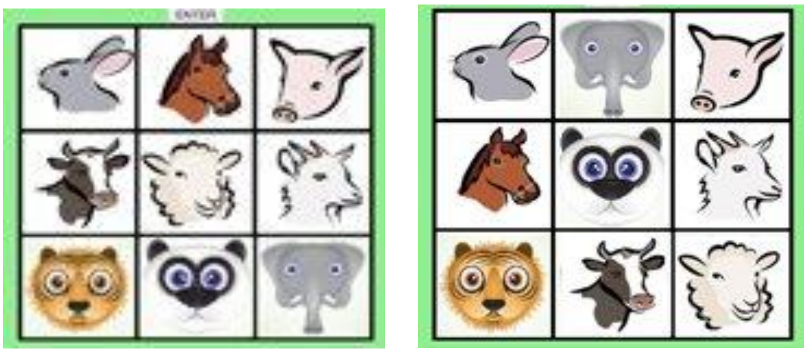

Image Sequencing fig 2 and 3

Here in fig n0.3, the position of the animals is 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 [3]:

1. Choose two large prime numbers eg. P and Q
2. Calculate N = P x Q
3. Select the general public key (i.e., Encryption Key) E such it's not an element of (P-1) and (Q- 1)
4. Select the Private key (i.e., Decryption Key) D such the subsequent 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 because 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

The strength of cloud computing is that the ability to manage risks especially to security issues. Security algorithms mentioned or encryption and decryption are often implementing in future to reinforce security over the network. In this, we will extend our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing. Cloud computing is defined because the set of resources or services offered through the web to the users on their demand by cloud providers. As each and each organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there's a requirement to guard that data against unauthorized access, modification or denial of services etc. 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.

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 signe with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing,“ in Proc. Parallel Distributed & 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.

[6]. 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.

[7]. Parsi Kalpana, Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, IJRCCT, ISSN 2278-5841, Vol.1, Iss:4, Sep 2012.

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

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

DOI 10.17148/IJARCCE.2020.9220