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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

To enhance the Reliability and Security in Cloud environment using RSA algorithm and Image Sequencing Password

Bohar Singh[1], Poonam[2], Aruna Rani[3]

Lecturer, CSE, SBSSTC, Ferozepur, India [1]

CSE, SBSSTC, Ferozepur, India [2]

Assistant Professor, ECE, SBSSTC, Ferozepur, India [3]

Abstract: Cloud computing is not something that suddenly appeared overnight. It may trace back to a time when computer systems remotely time-shared computing resources and applications. Cloud computing refers to the many different types of services and applications. These applications are delivered in the internet cloud. In the cloud computing the information is share between various users. Hence security and privacy are the two main challenges that are presents in the cloud computing. In our paper we are working on the security of cloud computing. To enhance the security of cloud computing, we are going to use RSA and image sequencing password.

Keywords*:* Security, RSA, Image Sequencing password, Attacks, Cloud Services.

I. INTRODUCTION

Now days, the computer technology is changed. The computer power, storage, and networking technologies are changed a lot. Cloud computing is acted as the large pool. In the cloud computing various accessible and virtualized resources are required. These resources include hardware, development platforms and services. [3] Cloud is an internet based technology uses the internet and central remote servers to support data and applications.

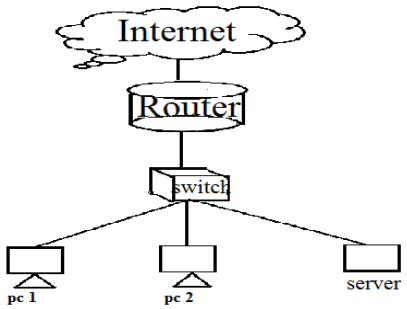

Fig 1: cloud computing in the form of internet

In the figure 1, the basic architecture of cloud computing is shown. As, in the front end, there are different PC's. These PC's are act as users. The switches and routers act as the intermediate between the internet and clients. And in the backend there is internet.

The cloud computing permits many user to access the system without installation personal files at any computer with internet access. In the cloud computing, the websites and server based applications were executed on a specific system [4]. The cloud computing is flexible in nature. The cloud computing flexibility is a function of the allocation of resources on authority request. The cloud computing provides the act of uniting. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet [5].

A. Service Models Of Cloud Computing:

Once a cloud is developed, it can be differ from its requirements. There is various models use in cloud computing.[3] These models are:

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.

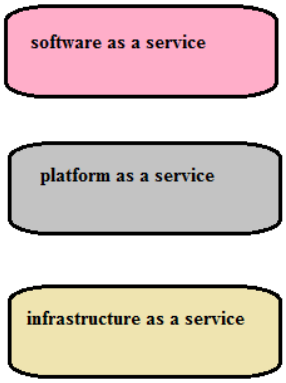

Fig 2: Service Models Of Cloud Computing

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.

DOI 10.17148/IJARCCE.2015.4616

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

B. Cloud Computing Using the Communications Services

In the cloud computing, the communication services can extend their capabilities. It helps to provides new interactive capabilities to current services. Cloud based communications services enable businesses to embed communications capabilities into business applications. The services of the cloud computing can be accessed from any location and linked into current services to extend their capabilities, as well as stand alone as service offerings.

C. *Accessing through Web APIs:*

Accessing communications capabilities in a cloud-based environment is achieved through APIs. It allows the application development outside the cloud to take advantage of the communication infrastructure within it.

D. *Security Threats Facing the Cloud***:**

There are many security threats available in the cloud computing.

Data Loss: Another serious threat stems from cloud computing service providers potential inability to prevent data loss.

Account Hijacking: Hijacking of accounts at cloud computing companies is another potentially serious threat. It is usually possible for authorized company personnel to remotely access cloud data via mobile devices or remote computers.

Insecure application programming interfaces (APIs):

Insecure application programming interfaces (APIs) are another threat to cloud computing. These interfaces offer ways for programs to communicate with each other and their security is not always completely guaranteed.

Denial of Service: Although it doesn't gravely affect integrity of the data stored in cloud computing servers, denial of service can temporarily deny access of data to legitimate users.

Data Handling: Sharing of technology and resources among different organizations always poses a risk to the data being handled. Sometimes servers at cloud computing firms are configured to work with data from few clients.

II. LITERATURE SURVEY

The Management of Security in Cloud Computing Ramgovind S, et.al,[2010]:

In this paper author discuss about the management of the cloud computing. Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization of data storage, of local networks as well as software Cloud computing[1] has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply. Using Cloud computing can help in keeping ones IT budget to a bare minimum. Cloud computing can deliver a vast array of IT capabilities in real time using many different types of resources such as hardware, software, virtual storage once logged onto a cloud.

Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, P. Syam Kumar et.al,[2010]:

In this paper author discuss about the data storage security in cloud computing. Cloud computing is an internet based computing. It delivers everything as a service over the internet based on user demand.[2] These services are classified into three types:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS).

Cloud data storage (Storage as a Service) is an important service of cloud computing referred as Infrastructure as a Service (IaaS). Data storage in cloud offers so many benefits to users. Cloud computing provides large amount of computing and storage to customers provisioned as a service over the internet. Cloud computing faces so many security challenges due to the many failures. In this paper, author focus on Ensuring data storage security in cloud computing, this is an important aspect of Quality of Service. In this paper, author propose an effective and flexible distribution verification protocol to address data storage security in cloud computing.

Above the Trust and Security in Cloud Computing: A Notion towards Innovation, Mahbub Ahmed et.al, [2010]:

In this paper author discuss the security of cloud computers. Cloud computing is for internet computing.[6] The internet is commonly visualized as clouds. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user. This paper shows the various cloud computing issues. To provide the best security to cloud computing author firstly derive a secure protocol by eliminating the dangling pitfalls that remain dormant.

An architecture based on proactive model for security in cloud computing, Prashant Srivastava et.al, [2011]:

In this paper, author discusses a proactive model for the security of cloud computing. Cloud computing is defined as a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud technology is a growing trend. Cloud Computing paradigm has one glaring problem: security, because the cloud is a new paradigm, it involves careful planning and execution. In this paper, author analyze the security landscape in detail and propose architecture based on a proactive model which tackles this increasingly difficult problem in a comprehensive manner.

Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, Cong Wang, Qian Wang, et.al,[2010]: In this paper author discuss about the data storage security in cloud computing. The cloud computing is the vision of computing as a utility, where users can remotely store their data into the cloud. Cloud Computing has been envisioned as the next generation

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

architecture of IT enterprise. Cloud Computing is transforming the very nature of how businesses use information technology.[7] One fundamental aspect of this paradigm shifting is that data is being centralized into the Cloud. In this paper author discuss about the data storage security. As the data of the user is very confidential in nature, so the data security has the main concern in cloud computing. There are many security reasons in the cloud computing, as: the infrastructures under the cloud are more powerful and reliable than personal computing devices. These devices are facing the both internal and external threats for data integrity. There exist various motivations for cloud service providers to behave towards the cloud users regarding the status of their outsourced data.

Data Security in Cloud Computing using RSA Algorithm, Parsi, Sudha Singaraju[2012]: In this paper author discuss about the cloud computing security. In the cloud computing security of the data is the major concern. Securing data is always of vital importance and because of the critical nature of cloud
and the large amounts of complex data it carries the need is even more important. Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. [8] Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user.

Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, Neha Tirthani Ganesan R: In this paper, author discuss about the data security in cloud computing. Now days, cloud computing becomes a difficult task. Cloud computing refers to a network of computers, connected through internet, sharing the resources given by cloud providers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. The security in cloud computing is the big issue. [9] The security threats such as maintenance of data integrity, data hiding and data safety dominate.

A Survey of Cryptographic Algorithms for Cloud Computing, Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh: In this paper, [10] author discuss about the cloud computing is the emerging field in the modern era. Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It conveys everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. Cloud computing conveys everything as a service over the web supports user demand. To secure the Cloud means secure the treatments and storage .

III. SECURITY ISSUES

In clouds data can be physically located anywhere in any data centre across the network 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. The cloud service provider for cloud makes sure that the customer does not face any problem 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. There are basic two types of attacks.

- Active attacks
- Passive attacks

In the passive attacks, the data is confidentially is breaks, as in this case the third party only access your data but the third party cannot do any modification in the data.

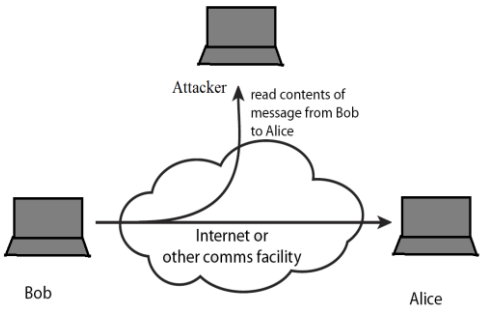

Fig 3: data confidentiality breaks

In the active attacks, the data integrity is breaks, the data can be modified by the third party and it send back to the user.

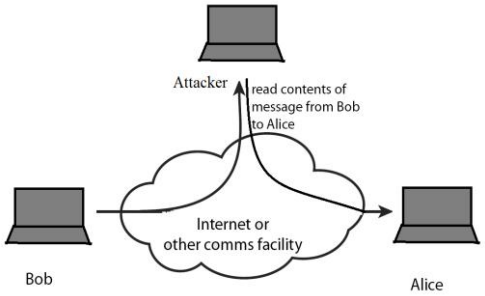

Fig 4: data integrity breaks

IV. PURPOSED WORK

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 entity is the one claimed
- Access Control - prevention of the unauthorized use of a resource
- Data Confidentiality –protection of data from unauthorized disclosure
- Data Integrity - assurance that data received is as sent by an authorized entity
- Non-Repudiation - protection against denial by one of the parties in a communication

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

In our case, we are going to use the image sequencing password with RSA to enhance the security of cloud computing. Suppose in this we have a sequence of horse-cow-goat-panda-1-6-U-Z. The sequence number of them is 24681548. So when we enter the sequence number we are enter to the cloud. Here we are going to use two images for image sequencing and each image contains 9 sequence. First diagram contain animals and second contains numeric and alphabets.

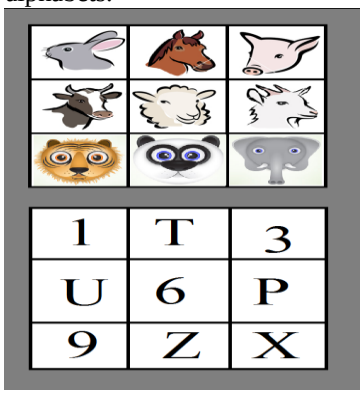

Fig 5: Image sequencing

Here in the figure 6, when you again get on this page or refresh the page your sequence will be changed and according to sequence your password is also changed. The position of the animals are shuffle, hence our password is also change. Now our password becomes 48653145 according to the position of horse-cow-goat-panda.

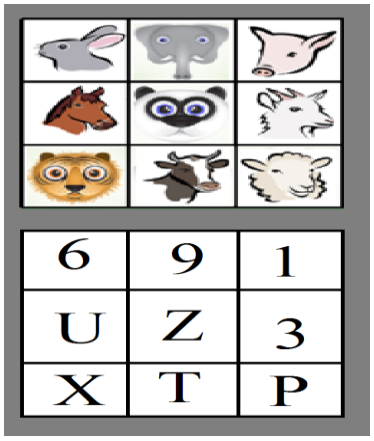

Fig 6: Image sequencing.

We are also 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:
   (D X E) mod (P-1) X (Q-1) = 1
5. For encryption, Calculate the cipher text CT from the plain text PT as follows:
   CT = PT^E mod N
6. Send CT as the cipher text to the receiver
7. For Decryption, Calculate the plain Text PT from the cipher text CT as follows:
   PT = CT^D mod N

V. RESULTS AND DISCUSSIONS

The work is done on the basis of novel approach which is built by the integration of authentication, image sequencing password and RSA algorithm. As we know that the data is stored on some else location in the cloud computing so we need high processing speed as well as high security. Here the graph shows the performance of our proposed scenario.

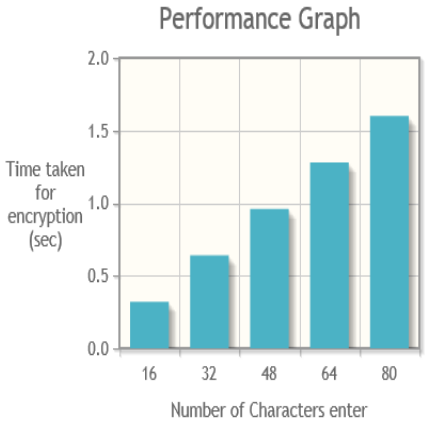

Fig 7: Performance Graph

Bars are showing that how much time it will take to encrypt data. Different experimental results are shown in the graph which are done on the basis of different experiments.

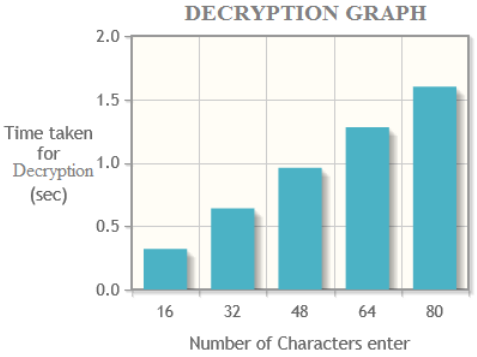

Fig 8: Performance Graph

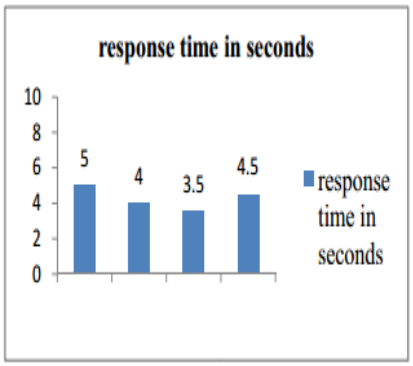

Fig 9: Base paper results

Now this graph contains the response time graph for their proposed scenario. At its y axes there are number of characters and the bars are showing time taken for encryption.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Table 1: Results comparison

Number of characters	Time taken by Proposed scenario	Time taken by previous scenario
10	0.2 sec	10 sec
20	0.4 sec	20 sec
30	0.6 sec	30 sec
40	0.8 sec	40 sec

Fig 10: Performance evaluation

As we know that the algorithms used in base paper are highly complex so they takes lots of steps and also time for encryption. But in our proposed schema the complexity of algorithm is not too much so it can provides much security in very less time as compare to base paper.

VI. CONCLUSION AND FUTURE SCOPE

Conclusion

The work is based on the enhancement of security and performance of cloud computing during network attacks. A novel approach is built by the integration of authentication, image sequencing password and RSA algorithm. The image sequencing password is dynamic in its nature, means it will change every time. It's integrated with RSA for encryption of data. Experiment is done in NetBeans using cloudsim simulator and results are shown in above section.

Future work

Every attack has its loop holes as well as every security mechanism also has some loop holes i.e. if attack is more powerful than it can bypass security. So to make system more secure we can some loop holes of recent attacks so that it does not allow them to bypass through security mechanism.

REFERENCES

[1] Ramgovind S, Eloff MM, Smith E, The Management of Security in Cloud Computing, 978-1-4244-5495-2/10/$26.00 ©2010 IEEE
[2] P. Syam Kumar, R. Subramanian and D. Thamizh Selvam ,Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010)
[3]. Introduction to Cloud Computing, a white paper
[4] .Cloud computing principles, systems and applications NICK Antonopoulos
[5] Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. (2009, Feb. 10). Above the clouds: A Berkeley
[6] Mahbub Ahmed, et.al, Above the Trust and Security in Cloud Computing: A Notion towards Innovation, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing
[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 for Cloud Computing , nternational Association of Scientific Innovation and Research (IASIR)