NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE2, Feb.-2016

INTRODUCTION OF TRUSTED COMPUTING PLATFORM IN CLOUD COMPUTING

Aayushi Bamboli
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Nilofar Tamboli,
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Pallavi Ghadage,
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Manisha Mohite,
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Sushila Kanade
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Guide-Prof: R. K. Narwade
BE(Computer Science & Engg.) JSPM'S BIT, Barshi

Special Thanks to
Dr.* Vyankatesh S. Kulkarni
Mechanical Engg. Department JSPM'S BIT, Barshi

ABSTRACT

We knew that cloud computing is could be usage of computer resources accessible via internet. Author has tried designing business model, which uses for divide and rule mechanism. Advantage of developed techniques is, by dividing the responsibility among different cloud services benefit to the clients. The implemented business model uses three sub models for encryption and decryption services, storage devices with CRM services. Both encryption and decryption data depends on cloud computing , the system administrator may simultaneously obtain both encrypted data and decryption keys to provide security authentication of user is done, invalid user is not allow to use the data. The major task in the implemented algorithm is uses of CRM for reduction of cost. Author proposed a secured cloud computing services through this paper. While implementing this algorithm own cloud environment is generated for security

purpose. The algorithm adopted is advanced encryption standard (AES) algorithm and service level agreement is used to improve the cloud security.

KEYWORDS: CRM, Cloud computing, data storage system, Encryption service, Decryption service

INTRODUCTION

In last few years cloud computing has gained a lot of importance and it is based on internet service. Main facilities of cloud computing is, it provides service for Storage, Infrastructure, Software and Providing Platform. The basic requirement of cloud computing it requires a computer with internet facility. In cloud computing, user is served with service as and when demanded for, Service may be Software, a hardware device needed for personal use or industrial (professional) use or a Storage needed for storing data. Cloud computing can be categorized in to two major sections, high scalability and high availability. The term availability means that the services are available even when quite a large number of nodes fail. There are many companies which provide cloud services e.g. Google, Amazon, Microsoft, and Salesforce.com.
Cloud computing can be categorized into two high scalability and high availability. Availability means that the services are available even when quite a number of nodes fail. Cloud services are provided by many IT companies like Google, Amazon, Microsoft, and Salesforce.com.

APPLICATION OF CLOUD COMPUTING

A. Software as a Service (SaaS) is a demanded model and offers an application. Eg: CRM, Google Apps, ERP etc. over the internet on demand. .

B. Platform as a Service (PaaS) this provider a complete solution for development platform. It has main advantage that, it includes the necessary services. e.g. Net Beans software, database, LDAP, MySQL, on the network and it can be avail any time.

C. Infrastructure as a Service (IaaS): Two different models are available in this layer, and this layer acts as an foundation layer. They foundation layer facilitates hardware and software infrastructure components. e.g. storage systems, computers etc. Recently national institute of standards and technology have identified three different models for cloud architecture as shown in fig no. 1.

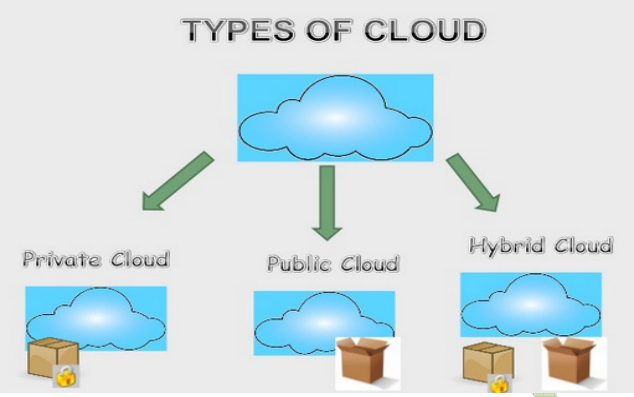

Fig. No.1. Cloud Architecture

A. Private Cloud: Private cloud can be set up in the small or large scale industry. Where cloud service provided and user will be working for same industry and cloud service is provided by the IT department of the same company. In short, the cloud service that can be used by internal units to deploy and run business applications.

B. Public Cloud: A public cloud can use by anyone whoever is able to use internet. And is aware of the specific cloud services. It can be used on demand.

C. Hybrid Cloud: It is a mixture of public and private cloud. e.g. if a industry designs a its own cloud to support and run business critical services and utilizes the public cloud for non critical services and for sharing less important information.

ENCRYPTION AND DECRYPTION

Encryption is the process of converting plaintext to cipher-text by applying mathematical transformations. These transformations are known as encryption algorithms and require an encryption key[2].
Decryption is the reverse process of encryption algorithm using decryption key. In Symmetric cryptology-Both key is the same as in symmetric or secret key cryptography. The key can different as in asymmetric or public key cryptography [3].

Types of cryptography
Symmetric cryptography uses the same secret (private) key to encrypt and decrypt its data.
Symmetric cryptography requires the secret key, there should mutual understanding between parties encrypting and decrypting data.

Asymmetric Cryptography uses two different keys i.e. public key and private key. Using the key they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key [1].

EXISTING SYSTEM

For achieving security in cloud, few technologies have been implemented for strengthening the mechanism for cloud computing. The other major services offered by cloud services are sending and understanding security message, it can also transport and manipulate by using web service tools. Security of the cloud system in still a big worry. The reason for this is trusted root environment for cloud computing is not been put in a clear way, many researchers are working on it and on almost each day some proposed system is coming. But practical implementation of proposed system is still a big question mark. As the cloud can be a public as we have stated earlier, if it is public cloud it is not safe.

PROPOSED SYSTEM

In this paper, author had been built a technique which can be used for establishing trusted environment for cloud computing system. This task is accomplished by integrating the trusted computing platform into cloud computing system. While implementing this paper AES type of algorithm is used and also made provision for usage of RSA algorithm. Author has developed a model, which can be used for cloud computing and it is combine with trusted computational platform. In the proposed system trusted platform module is also used in conjunction with trusted computational platform for adding security to cloud storage.

AES (advance encryption Standard algorithm):

AES algorithm is symmetric cryptography example. In this only one key is used i.e. shared key. Provide security to the information and data processing system.AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits. In this same key is used by sender and receiver while encrypting and decrypting. So receiver must know the secret key.

AES algorithm and creating cloud environment secure our data. In addition it's difficult to the hacker to break our code as we are giving secret id for each registering entry.

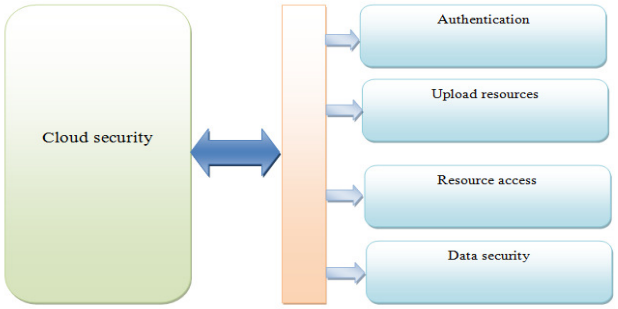

Fig. System Architecture

CONCLUSION

Three services are provided by cloud Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud service can be accessed by a device that can access the internet; the device may be Laptop, PC and Smart Phone etc. A Cloud computing, all users data is encrypted and stored in Cloud service provider.

The main aim of this paper is dividing of authority to reduce operational risk due to which unauthorized access of data.

REFERENCES

Text references

[1] G. Frankova, Service Level Agreements: *Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.*

[2] A.R. Kamble, Sanket Taral, Prasad Kubade, Abhishek Wagh, Nikhil Shete, "*Business model based on separate encryption and decryption services".*

Net References

[3]"*Service Level Agreement and Master Service Agreement", http: //www. Soft layer. Com/ sla.html, accessed on April 05, 2009.*

[4] "*Sampling issues we are addressing", http://cloudsecurityalliance.org/issues.html#15, accessed on April 09, 2009.*

[5] S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "*Security for the cloud infrastructure: trusted virtual data center (TVDc)." [Online]. Available: www.kiskeya.net /ramon/work/pubs/ibmjrd09.pdf*