SECURITY ALGORITHM IN CLOUD COMPUTING: OVERVIEW

M. Vijayapriya
M. Phil. Research Scholar,
PG & Research Department of Computer Science,
Government Arts College, Coimbatore-18.
avp.priya@gmail.com

Abstract*:* Network security is becoming more and more important as people spend more and more time connected. It is a specialized field in computer networking that involves securing a computer network infrastructure. It is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access. It also ensures that we have an adequate access to the network and resources to work. A network security system typically lies on the layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and the appliances. All components work together to increase the overall security of the computer network. For enhancing the security, many algorithms are widely used. Cloud Computing is a set of IT based Services that are provided to a customer over a network and these services are delivered by a third party provider who owns the infrastructure. It is often provided "as a service" over the Internet and that was typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), data storage as a service (DSaaS). This research paper presents what cloud computing is, security algorithms and the challenges in cloud computing.

Keywords: Cloud computing, Security algorithms, Encryption, Decryption.

I. INTRODUCTION

Internet has been the driving force that towards various technologies have been developed. In that one of the most discussed is cloud computing. Cloud Computing [1, 2] is an emerging trend to deploy and maintain software and is being adopted by the industry such as Google, IBM, Microsoft, and Amazon. Several prototype applications and platforms are used, such as the IBM — Blue Cloud infrastructure, the Google App Engine, the Amazon Cloud, and the Elastic Computing Platform. As the use of these services becomes widespread, then the security of outsourced user data becomes an important research topic. This paper describes the overview of cloud computing, algorithms used and its security concerns.

In cloud computing, there are many data privacy concerns. Improper disclosure of a business data to third parties is one of the major concerns realized. Encryption should be properly used and the existing methods include FIPS, TDEA, AES, RSA and ECC. In this paper, we describe about using algorithms and the enhancement of security concern.

II. CLOUD COMPUTING: OVERVIEW

Cloud computing is the hottest topic in the IT & research today. It is a new computing model in which the resources are pooled to provide software, platform and infrastructure to as many users as possible by sharing available resource. It is continuously evolving and there are several major cloud providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) and we discuss some of the services that are being provided. There are many scholarly researches, articles and periodicals on cloud computing security concern out there.

III. CLOUD COMPUTING BUILDING BLOCKS

Cloud computing is actually a combination of various computing techniques like virtualization, distributed computing, load balancing etc. The building blocks of cloud computing are as follows:

A. Deployment Models:

Deployment model is that the cloud can be deployed for private, public, community or uses. It consists of Private cloud, Public cloud, Community cloud and hybrid cloud.

Private cloud:

Private cloud is used by an organization and its customers, who own it. Its infrastructure is operated solely for a particular organization. It may be managed by the organization or a third party. In the private cloud, scalable resources and the virtual applications that are provided by the cloud vendor are pooled together and that is available for cloud users to share and use. Only the organization and members may have access to operate on a specific Private cloud. **Example:** Eucalyptus Systems.

Public cloud:

Public cloud is made available for the use of public. It describes basic traditional mainstream sense, whereby it provides self-service basis over the internet. It is mainly based on a pay-per-use model, that was similar to a prepaid electricity metering system that is flexible and enough to cater for spikes in demand for cloud optimization [3]. Public clouds are less secure when compared to other cloud models because it places an additional burden that is all applications and data accessed on the public cloud are not free from malicious attacks. **Example:** Microsoft Azure, Google App Engine.

Community cloud:

Community cloud is for a community of users who are having same mission or goal. The infrastructure is shared by several organizations for a shared cause. It is managed by them or a third party service provider. These clouds are normally based on an agreement. In this environment, operating cloud may exist locally or remotely. Example: Face book.

Hybrid cloud:

Hybrid cloud shares the properties of any of the above mentioned models. It is a private cloud linked to one or more external cloud services. It is centrally managed, provisioned as a single unit, and circumscribed by secure network [4]. It is a mix of both public and private clouds. This Cloud provides more secure control of the data and applications. And also it allows to various information over the Internet. It is an open architecture and that allows interfaces with the other management systems.

Example: Amazon Web Services (AWS).

B. Delivery Models:

The cloud delivers it’s outsource services in the form of software, platform and infrastructure. There are some costly applications like ERP, CRM etc. that will be offloaded onto the cloud by provider. These applications run at providers cost.

C. Hallmarks of cloud:

The cloud services that to use needn’t be paid in advance. It provides the services on demand. These services are almost available on any Internet enabled device that is having browser software installed in it. The cloud providers pool the resource from various resources and make these services.

D. Service Models:

Based on the different types of services provided, it can be considered that cloud computing consist of three main service models such as:

1. *SOFTWARE AS A SERVICE (SAAS):*

Software as a Service (SaaS) is the topmost layer which features a complete application that was offered as a service on demand. It can be described as a process by which Application Service Provider (ASP) provide many different software applications over the Internet. This service makes the customer to get rid of installing and operating the application on own computer. SaaS vendor takes responsibility for deploying and managing the IT infrastructure and processes required to run and manage the full solution. SaaS features a complete application offered as service on demand. In SaaS, there is Divided Cloud and Convergence coherence mechanism in that every data item has either the ―Read Lock‖ or ―Write Lock‖ [5]. Two types of servers are mainly used by SaaS: The Main Consistence Server (MCS) and Domain Consistence Server (DCS).

2. *PLATFORM AS A SERVICE (PAAS):*

Platform as a service (PaaS) is the delivery of a computing platform and solution stack as a service without software downloads or installation for end-users. It provides an infrastructure with high level of integration. That is mainly in order to implement and test cloud applications. The user does not manage the overall infrastructure (including the network, servers, operating systems and storage), but he controls deployed applications and their configurations. **Examples**: Force.com, Google App Engine and Microsoft Azure.

3. *INFRASTRUCTURE AS A SERVICE (IAAS):*

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services. It can be done by using Virtualization technology. Its main objective is to make resources such as servers, network and storage that are accessible by applications and the operating systems. Examples: Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

IV. SECURITY ALGORITHMS

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption.

1. RSA

This algorithm is used for public-key cryptography. It is the first and still most commonly used asymmetric algorithm. It involves two keys- a public key and a private key. The public key is used for encrypting messages and known to all. Messages encrypted with the use of public key can only be decrypted by using the private key.

In this authentication scheme, the server implements public key authentication by signing a unique message with its private key, thus creating what is called digital signature. The signature is then returned to the client. Then it verifies using the server's known public key [6].

2. MD5- (Message-Digest algorithm 5)

A widely used cryptographic hash function algorithm with a 128-bit hash value and processes a variable-length message into a fixed-length output of 128 bits. First the input message is broken up into chunks of 512-bit blocks then the message is padded so that its total length is divisible by 512. In this, the sender of the data use the public key to encrypt the message and the receiver uses its private key to decrypt the message.

3. AES- Advanced Encryption Standard (AES)

It is a symmetric-key encryption standard. It uses 10, 12, or 14 rounds. Each of the ciphers has a 128-bit block size, with the key sizes of 128, 192 and 256 bits, respectively [7]. It ensures that the hash code is encrypted in a highly secure manner. Its algorithm steps are as follows:

1. Key Expansion
2. Initial round
3. Add Round Key
4. Rounds
5. Sub Bytes
6. Shift Rows
7. Mix Columns
8. Add Round Key
9. Final Round
10. Sub Bytes
11. Shift Rows
12. Add Round Key.

V. CONCLUSION

The strength of cloud computing is the ability to manage risks in particular to security issues. Security algorithms mentioned for encryption and decryption can be implementing in future to enhance security over the network. In the future, we will extend our research by providing algorithm implementations and producing results to justify our concepts of security for cloud computing.

REFERENCE

[1] Anthony Bisong, Syed, M. Rahman "An overview of the security concerns in Enterprise cloud computing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[2] I. Foster, Y. Zhao, I. Raicu, and S. Lu, 2008, "Cloud Computing and Grid Computing 360-Degree Compared, In: Grid Computing Environments Workshop", 2008. GCE '08, p. 10, 1.

[3] Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, June 2011.

[4] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL", Research Journal of Applied Sciences, Engineering and Technology, 2012, ISSN: 2040-7467.

[5] Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, ―SaaAS – "The Mobile Agent based Service for Cloud Computing in Internet Environment", Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, 2010. ISBN: 978-1-4244-5958-2.

[6] Andrea Pellegrini, Valeria Bertacco, "Fault-Based attack of RSA Authentication".

[7] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[8] K.S.Suresh, Prof K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing", 2012, Volume 2, Issue 10, October 2012.