IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.117109

# The Scope and Research on Cloud Computing Security

**Emmanuel R[1], Chandrashekar C M[2], Laxmidevi H M[3], Purushotham Sharma R[4]**

Associate Professor, ISE Department, R R Institute of Technology, Bangalore, India[1]

Assistant Professor, CSE Department, R R Institute of Technology, Bangalore, India[2,3]

UG Student, ISE Department, R R Institute of Technology, Bangalore, India[4]

**Abstract:** Cloud computing has grown rapidly in recent years as a novel method. However, because security concerns have had a significant impact on the development and adoption of cloud computing, its importance and urgency must not be overlooked. This paper introduces cloud computing and its security situation, studies the main security problems of cloud computing, and proposes a cloud computing security framework that can effectively solve these security problems. It also points out that cloud computing can continue to expand, and its applications will become more and more widespread, if only the security problems are solved.

**Keywords:** Scope of Cloud Computing Security, Cloud Computing Security, Research on Cloud Security, Future of Cloud Security.

## I. INTRODUCTION

Cloud computing is a novel technology that is based on distributed processing, parallel computing, and grid computing, and it is one of the most talked-about subjects in the field of information technology. It has attracted the interest of academic circles, business circles, and governments.

A SaaS provider often hosts and administers an application in their own data center and makes it available via the Internet to many tenants and customers. Some SaaS providers use PaaS or IaaS services from another cloud provider. Salesforce.com and Oracle's CRM on Demand are two well-known SaaS examples. PaaS is a Web-based application development and deployment platform that is provided as a service to developers. This platform is made up of infrastructure software, such as a database, middleware, and development tools. Google App Engine and Engine Yard are two well-known PaaS service providers. The distribution of hardware and accompanying software as a service is known as IaaS. It's a step forward from traditional hosting in that it doesn't require a long-term commitment and allows customers to deploy resources as needed. IaaS services include Amazon Web Services' Elastic Compute Cloud (EC2) and Secure Storage Service (S3).

## II. CLOUD COMPUTING SECURITY FRAMEWORK

Cloud computing is now experiencing numerous security issues, which are posing a barrier to its development and adoption. As a result, a cloud computing security framework must be developed, as well as active cloud security core technology research. We offer a cloud computing security architecture in this paper.

**Firewall**

It can considerably improve the security of a firewall configuration for cloud computing. Limiting the type of open port is the method. The Web server group, for example, opens ports 80 and 443 to the world, whereas the application server group only opens port 8000 (special application service ports) for the Web server group and the database server group only opens port 3306 (MySQL port) for the application server group. Simultaneously, the three sets of network servers open port 22 (SSH port) for clients and refuse all other network connections by default. The security will be substantially enhanced by this approach.

**Security Measure for SaaS**

SaaS providers in cloud computing should provide consumers with complete applications and components, as well as guarantee programme and component security. There are two primary components to the proposed security functions:

Priority access control strategy: SaaS providers typically provide Identity identification and access control in the form of a user name and password verification system.

Users should be familiar enough with the provider they have chosen to eliminate the threat to the internal security of cloud apps. At the same time, cloud providers should provide high strength, change passwords on a regular basis, base password length on critical data, and not use functions like previous passwords to increase user account security.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.117109

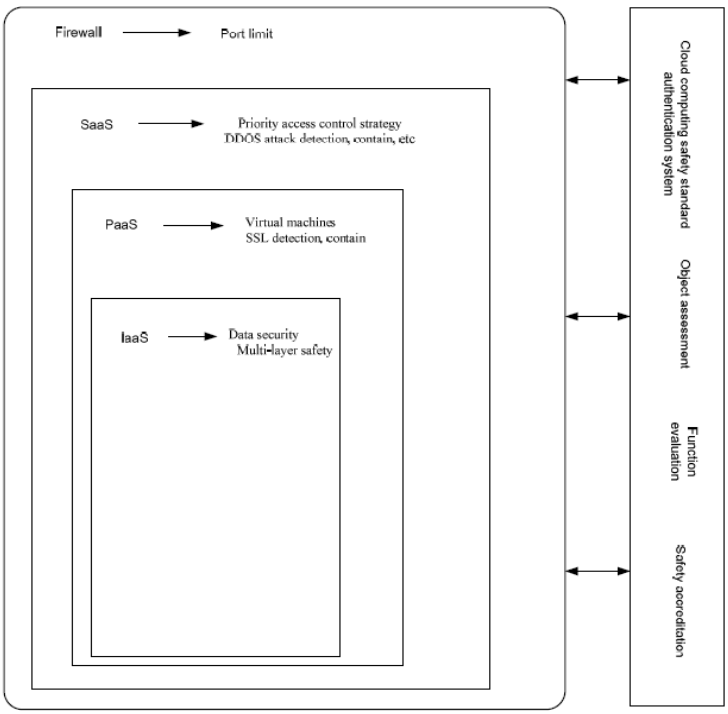


**Figure 1:** Security Measures on Different Services

**Security Measures of PaaS Layer**

PaaS is the intermediary layer in cloud computing, and security measures are divided into two categories:
Application of virtual machine technology: Virtual machine technology allows providers to set up virtual machines in existing operating systems. Set access limitations at the same time, so that regular users can only operate computer hardware by encouraging operational permissions. This clearly distinguishes between ordinary users and administrators; even if a user is attacked, the server will not be harmed.

SSL attack defence: If an SSL attack is conceivable, the user must improve the prevent technique. Providers should give the necessary patch and precautions so that users can patch for the first time and ensure that the SSL patch works promptly. Using the firewall to block particular ports to prevent common HTTPS assaults, strengthening management authority, and making security certificates difficult to obtain are all strong defence tactics.

**Security Measures of IaaS Layer**

In general, IaaS is not accessible to ordinary users; management and maintenance are also fully dependent on cloud providers, and data security is the most crucial aspect. Cloud providers should inform users about the country in which the server is located, and it should be easy to operate this data without violating local legislation. Because data encryption is not only reliable but also reduces data efficiency when combining distinct user data, providers must divide user data kept on multiple data servers. Data separation chaos can be avoided by separating user data storage. Important and secret data should be backed up at the same time, so that data can be easily recovered in the event of a hardware breakdown.

## III. CLOUD COMPUTING STANDARD AUTHENTICATION

Cloud computing currently lacks a unified security standard authentication system, but many organizations have been established to set the standards. A complete set of cloud computing security frameworks requires reference standards, which can be used to assess the framework's integrity, function, and security. The system is reliant on the advancement of the unified cloud computing security standard, which, as previously said, is a set of comprehensive security authentication standards aimed at solving cloud computing's many security issues.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022
DOI: 10.17148/IJARCCE.2022.117109

## IV. DATA SECURITY OF CLOUD COMPUTING

Customers don't know where their data is stored on servers when they utilize cloud computing services, and they don't even know which nation these servers are in. When these countries need to investigate these data, providers may be required to give data and may be unable to ensure the security of user data due to differing laws.
Data separation: A considerable volume of user data is stored in a shared environment in cloud computing services. In order to save money, ISPs frequently reuse IP addresses; another, resulting in data misuse, may use an IP address from one user. There is no guarantee of data privacy.
Data separation: A considerable volume of user data is stored in a shared environment in cloud computing services. In order to save money, ISPs frequently reuse IP addresses; another, resulting in data misuse, may use an IP address from one user. There is no guarantee of data privacy. Data encryption is one approach to protect data security, although encryption does not always guarantee data security, and a failure of decryption might result in data destruction. Users and cloud services are unable to access data, which diminishes data efficiency and wastes resources.

## V. CONCLUSION

Cloud computing has grown in popularity in recent years, but security issues have become challenges that must be overcome in order for cloud computing to become more widely used. This article examined the current state of cloud computing development as well as security issues, and offered a cloud computing security reference model. The model proposed a number of answers to the current security issues that cloud computing encounters, but technology implementation will require additional firms and individuals to participate in cloud computing security research. At the same time, cloud-computing security is more than a technical issue; it also involves standardization, supervision, laws and regulations, and a variety of other factors. Cloud computing also brings with it development opportunities and challenges, in addition to the security issue.
.

## REFERENCES

[1] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009)
[2] Amazon Web Services. Amazon Virtual private Cloud, http://aws.amazon.com/vpc/
[3] Catteddu, D.: Cloud Computing: Benefits, Risks and Recommendations for Information Security. CCIS, vol. 72, pp. 50–56 (2010)
[4] Amazon Web Services. Overview of Security Processes, http://aws.amazon.com/ec2
[5] Bikram, B.: Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing 4, 34–35 (2009)
[6] Boss, G., Malladi, P., Quan, D., et al.: IBM Cloud Computing White Book http://www-01.ibm.com/software/cn/Tivoli/ao/reg.html
[7] Jamil, D., Zaki, H.: Cloud Computing Security. International Journal of Engineering Science and Technology 3(4), 3478–3483 (2011)
[8] Zhang, S., Zhang, S., Chen, X.: Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks, ICFN 2010, p. 93 (2010)
[9] Shen, Z., Tong, Q.: The security of cloud computing system enabled by trusted computing technology. In: 2nd International Conference on Signal Processing Systems (ICSPS 2010), vol. 2, pp. 2–11 (2010)
[10] Somani, U., Lakhani, K., Mundra, M.: Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing.