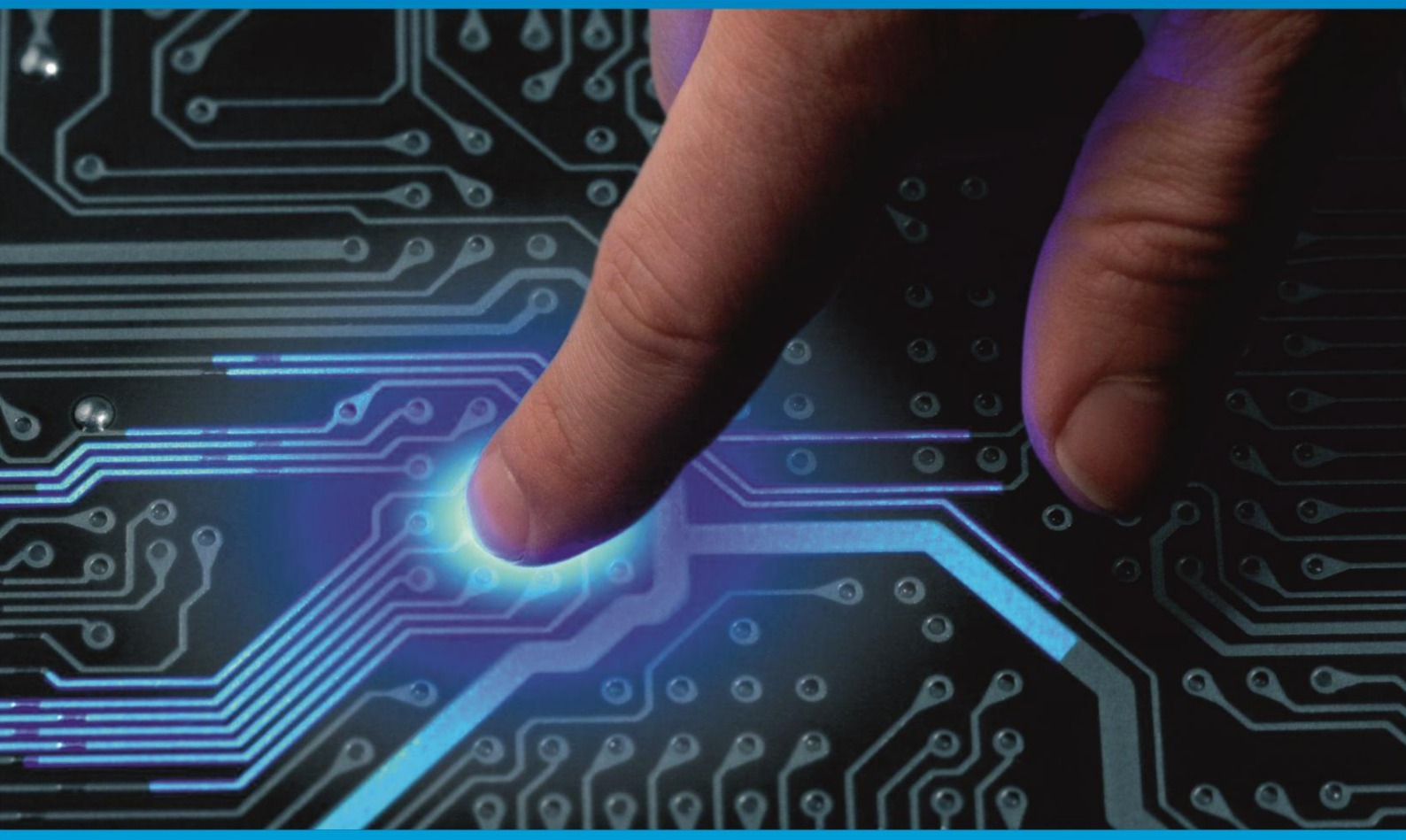
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

# Overview on Security Issues in Cloud Computing

**Swathi Pothuganti**

Lecturer, Department of Computer Science, Sreechaitanya Degree College, Telangana, India

**ABSTRACT:** Inside the ongoing decade, significant developments in technology have arisen that possibly add more accommodation to everyday life rehearses on an enterprise-level as well as on a singular level also. Cloud Computing technology has seen huge advances in its execution and becomes broadly received by one or the other private or public areas. It was clear as of late that many associations and enterprises are moving their outstanding tasks at hand to the cloud. In any case, Security is a significant worry for the cloud computing administrations, which depends on the Internet association that makes it powerless against numerous kinds of attacks. Despite the fact that that the security estimates executed over cloud computing are building up each spending year, Security still a test. In this paper, we led a review concentrate on cloud computing and tended to various kinds of attacks and potential dangers to this arising technology, just as assurance strategies and existing answers for such attacks.

**KEYWORDS**: Cloud Computing, Information Security, Cyberattacks, Threats

## I. INTRODUCTION

Cloud computing (CC) technology has been extensively used in numerous territories, including document sharing, ongoing applications, and correspondence. Significant CC advancements have arisen ongoing many years, including critical advances. CC has become generally received in both the private and public areas due to the common sense of its services, which can conceivably add comfort at a few levels. Then again, the Security of the offered types of assistance is an essential worry for both cloud clients and cloud service suppliers [1]. Cloud Computing security is a basic subdomain of PC security, and it represents a significant test to cloud advancements' broad appropriation. Since CC services are basically dependent on an Internet association, they are helpless to an assortment of attacks and other security dangers, which can bring about possibly extreme effects, for example, information breaks, malware infusions, denial-of-service (DoS) attacks, information misfortunes, and unreliable application programming interfaces (APIs). As indicated by, security occurrences in the cloud climate have developed outstandingly over a couple of past years, presumably due to the striking development in cloud services. For this paper, we directed a review on Cloud Computing to address different kinds of attacks and different dangers to this advancing technology, just as potential insurance techniques also, the current answers for such issues.

## II. OVERVIEW ON CLOUD COMPUTING

Cloud Computing is characterized by the National Institute of Standards and Technology (NIST) as "A model for empowering pervasive, helpful, on-request network admittance to a common pool of configurable computing assets (e.g., networks, workers, stockpiling, applications, and services) that can be quickly provisioned and delivered with insignificant administration exertion or service supplier communication."This segment gives a short review of CC technology, counting its engineering, service models, organization models, and preferences, and detriments[2]. The fundamental CC attributes are represented in the accompanying subsection.

### *The architecture of Cloud Computing*

The cloud architecture is generally classified into three cloud service models: infrastructure-as-a-service (IaaS), the most minimal layer, which gives fundamental infrastructure to different layers; platform-as-a-service (PaaS), the middle layer, which gives an environment to creating and facilitating users' applications; and software-as-a-service (SaaS), the upper layer, which gives an application layer that works as a service on demand.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

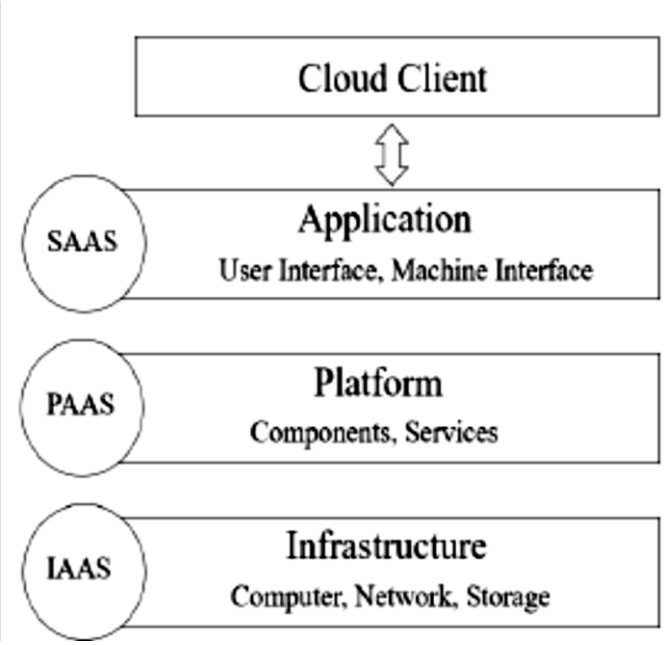



**Figure 1:Service Model in Cloud Architecture**

**Software-as-a-Service (SaaS)**

SaaS is also known as an on-demand service that allows customers to use applications that are facilitated on a cloud worker and conveyed over the Internet; this can incorporate on the web office suites and email applications. Users can buy into online software services to handle their business' requirements at a small expense instead of purchasing a new software[3]. The customers rely upon the suppliers for Security. SaaS doesn't need the users to have special hardware or software; notwithstanding, it requires a permanent Internet association.

**Platform-as-a-service (PaaS)**

PaaS, the layer beneath SaaS, allows developers to proficiently compose and create SaaS applications and send them on the PaaS layer. PaaS totally bolsters the software life cycle, and it is an economical alternative for developers, as it allows them to concentrate on building and running applications rather than on observing the hidden infrastructure[4]. The service suppliers are answerable for building and maintaining the infrastructure for the developers.

**Infrastructure-as-a-service (IaaS)**

IaaS, the least layer, gives the fundamental infrastructure to the above layers. IaaS incorporates networking hardware, servers, operating systems (OS), and storage. It allows buyers to use total assets without purchasing physical hardware. IaaS is also a cost-successful and faster decision for operating the workload without the need to purchase or, on the other hand, manage the hidden infrastructure[5].

## III. DEPLOYMENT MODEL OF CLOUD COMPUTING

There are four main arrangement models for Cloud Computing proposed by NIST, public clouds, private clouds, hybrids clouds, and community clouds.

**1. Public Cloud**

In a public cloud environment, hardware and software assets are publicly shared among various users. A third party public cloud service supplier manages and screens this environment, so such clouds are suitable for the information that isn't sensitive[6].

**2. Private Cloud**

A private cloud is operated by a solitary organization; all of a given cloud's systems and services are just accessible inside the boundaries of that organization.

The company handles all the management and maintenance related to the infrastructure; a private cloud is subsequently extravagant. However, it is safer than a public cloud.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

**3. Hybrid Cloud**

A hybrid cloud is a combination of at least two sorts of clouds (e.g., a public-private cloud). Because it shows the features of the elaborate clouds, this sort of deployment model gives high scalability and adaptability, as well as many choices for data deployment. A hybrid cloud is managed centrally[7].

**4. Community cloud**

Community clouds are similar to public clouds in many aspects; notwithstanding, this cloud-service model is usually expected for explicit individuals, organizations, or organizations that share the same cloud prerequisites. In a community cloud, by the same token participating community individuals or an outsider service supplier can manage the shared assets.

## IV. SECURITY IN CLOUD COMPUTING

**1. Cloud Computing Security Requirements**

Confidentiality requires hindering unauthorized exposure of CC service users' information. Cloud suppliers charge users to guarantee confidentiality; in CC, the attention is on authentication of cloud assets (e.g., requiring a username and password for each client). Besides, Availability is the ability for the shopper to use the framework as anticipated. A customer's Availability may be guaranteed as one of the details of a contract; to guarantee Availability, a supplier may make sure about immense capacity and magnificent architecture. Accountability includes checking the customers' various activities in the data clouds. Accountability is achieved by checking the information that each customer supplies (and that is signed in various places in information clouds).

**2. Classification of Cloud Security Issues**

CC contains many categories, each of which has many security concerns. The security issues happen all through CC hardware, software, and communication. Data absconds in cryptographic strategies can cause security issues in data focuses or in communication. These issues can also come from the client if the authentication strategy is weak[8].

**A. Embedded Security**

Embedded systems have the advantages of top-notch devices and require the client to interface with a local network to open the troubleshoot ability. The main CC security issues in the embedded framework are because of the utilization of VMs. Such systems have the advantages of solidarity and isolation. In any case, a VM can have a real security threat when an issue with deployment happens. Data leakage can arise through the implementation of separate VM workloads. In this way, CC suppliers should be careful when uploading isolated VMs into the infrastructure. In addition, in VM checking, the host PC works as a controlling point, as the host machine can update and change any assets in the VM.

**B. Application**

The most touchy and vulnerable areas of any framework are software applications. The software incorporates both a front end and a back end on many platforms and frameworks. The enormous amount of software code is the primary cause of security concerns[9]. At the point when an application has many programmers and/or coding languages, many vulnerabilities can arise.

**C. Client Management**

Client management is a security matter in the CC environment. Client management just includes securing the public information in the customer's framework. The customer's experience plays an important part in a cloud, as cloud services are developing quickly to the point that the business is encountering an overall service increase. That's the reason a few suppliers are battling because of the deployment of weak answers for the client. A few users with involvement with the cloud security field will battle while choosing a cloud supplier. Client authentication plays a great part in shielding the cloud from carefully illegal access.

**D. Cloud Data Storage**

The most significant part of CC is cloud data storage. Given the current development in online applications and the associated gadgets, the security issues related to cloud data storage are getting more important. Data warehouse deployment requires high Security, which mirrors the quality of the cloud service.

**E. Cluster Computing**

A computer cluster includes various computers, VMs, or servers that are associated together to run as a solitary framework. Industrial CC utilizes the idea of clustering for parallel handling. This method has many advantages, yet it can cause security challenges because of the increase in users in each cluster.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

## V. ATTACKS AND COUNTERMEASURES IN A CLOUD COMPUTING ENVIRONMENT

The vital motivation of this research is to decide the potential attacks in the CC environment and their possible arrangements. CC offers services utilizing IaaS, PaaS, and SaaS, as appeared in Figure 1. In this paper, we classified the attacks based on the service conveyance model of CC.

### 1. Security attacks on SaaS cloud layer

In SaaS, most users are as yet uncomfortable with the SaaS model because of data-related security issues, for example, who possesses the data, data backup, data access, data locality, data availability, personality management, and authentication. We consider famous sorts of security attacks on the SaaS cloud layer, as elaborated below.

### A.Denial of service (DoS) attacks

DoS attacks are the most noticeable attacks in the CC environment. The main aim of the attacker is to exhaust all the assets of the casualty by sending thousands of solicitation packets to the casualty over the Internet. In fact, the rate of DoS attacks is increasing because of certain characteristics of CC, for example, on-demand services, self-service, and broad network access. DoS attacks target the Availability of the services gave by the cloud to flood a network. Along these lines, they decrease the client's bandwidth, upset service to a particular framework, and keep the client from accessing or utilizing the cloud service[10]. There are many types of DoS attacks, such as Distributed DoS (DDoS) attacks, which are extended from DoS attacks and involve the attacker using numerous network hosts to inflict more devastating effects on the victim.

### B. Authentication attack

The character is utilized to identify users to achieve secure access to cloud applications. Fundamentally, the personality is the center part of any virtualized CC framework. For sure, authentication attacks can delicately happen in cloud environments because of the weak mechanism of username and password that users actually utilize. Thus, authentication cloud attacks, for example, animal power and dictionary attacks, are the most common. In this attack, the attackers target the mechanisms utilized by the client to authenticate the framework.

### 2. Security attacks on PaaS cloud layer

In PaaS, the client controls the applications that run in a cloud environment; however, the cloud supplier controls the hardware, network base, and operating systems. Nonetheless, lack of validation, anonymous signs, and service fraud are major issues in PaaS. We talk about famous sorts of security attacks on the PaaS cloud layer below.

### A. Phishing attacks

Phishing attacks affect the two suppliers and users in the PaaS cloud model. This kind of attack aims to recover personal information from a legitimate client by manipulating a web connect and diverting the client to a spoofed interface[11]. In CC, phishing attacks can be classified into two categories. The main is abusive behavior, in which an attacker hosts a phishing attack site on the cloud by utilizing one of the cloud services; the second includes hijacking the accounts utilizing traditional social designing techniques.

### B. Port Scanning Attack

The port scan is a famous attack. The main aim of a port scanning attack is to access the assets in a cloud network. In this attack, the attacker utilizes open ports address that has a place with an association with gain exact information about the working environment and running application measures. Subsequently, the attacker misuses this information and endeavor the vulnerabilities to play out the actual attack since it's executed after the scanning port phase.

### 3. Security attacks on IaaS cloud layer

The security worries at the virtualized level are major protections threats to the IaaS computing environment. As recently examined, in CC, available infrastructures incorporate an assortment of several computers, VMs, and storage assets to store important information, for example, confidential information and data reports. On this layer, the engineer has better command over the Security because there is no security opening in the virtualization manager[12]. Besides, sharing the physical assets of a host among virtual machines through a hypervisor abstraction layer is enabled by virtualization. We describe some major security attacks on the IaaS cloud layer, as elaborated below.

### A. Cross-virtual-machine attacks (Side-channel attacks)

In the cloud environment, virtual machines (VMs) are easily accessible by the tenant users. Accordingly, they are the most vulnerable part of the virtualized framework. Side-channel attacks are likely one of the most challenging sorts

of attacks in a cloud environment. These attacks are meant to extract confidential information from a casualty's VM by misusing side-channel information, for example, time, cache, heat, and force. This information is recovered from the cryptographic software that is neither the plaintext to be scrambled nor the code text coming about because of the encryption cycle[13]. Placement and extraction are the main strides in side-channel attacks.

**B. VM rollback attack**

Basically, in a VM rollback attack, the attacker takes advantage of a VM from an old snapshot and runs it without the client's awareness. The attacker can get the password for the VM by launching a savage power attack, regardless of whether the visitor operating framework has a limitation on the quantity of failed trials. In addition, the attacker can change users' consents utilizing rollback, an authorization control module.

## VI. CONCLUSION

Cloud Computing security is an essential aspect of computer security, and it poses a major challenge to its widespread adoption because the fact that CC services are essentially based on Internet association makes them vulnerable to a variety of attacks and security threats that may result in the same token light or extreme impacts. In this paper, we investigated the significant attacks threatening the Security of Cloud Computing; besides, we gave arrangements and possible countermeasures to fill in as a kind of perspective for comparative analysis.

## REFERENCES

[1] M.Rajendra Prasad, Dr.Jayadev Gyani, Dr.P.R.K.Murti, "Mobile Cloud Computing Implications and Challenges", IISTE Journal of Informational Engineering and Applications (JIEA); http://iiste.org; pp.7-15, Vol.2, No.7, 2012.

[2] Okuhara, M., Shiozaki, T. and Suzuki, T. (2010). Security Architectures for Cloud Computing. FUJITSU Science Technology Journal, 46(4), 397–402.

[3] Vishal Dineshkumar Soni. (2018). IOT BASED PARKING LOT. International Engineering Journal For Research & Development, 3(1), 9. https://doi.org/10.17605/OSF.IO/9GSAR

[4] Soni, Vishal Dineshkumar and Soni, Ankit Narendrakumar and POTHUGANTI, KARUNAKAR, Student Body Temperature and Physical Distance Management Device in Classroom Using 3d Stereoscopic Distance Measurement (2020). International Journal of Innovative Research in Science Engineering and Technology 9(9):9294-9299,

[5] Rashmi, Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401

[6] Ankit Narendrakumar Soni (2019). Spam-e-mail-detection-using-advanced-deep-convolution-neural-network-algorithms. JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE, 2(5), 74-80.

[7] I. Ahmad and K. Pothuganti, "Design & implementation of real time autonomous car by using image processing &IoT," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 107-113, doi: 10.1109/ICSSIT48917.2020.9214125

[8] Soni, Ankit Narendrakumar, Diabetes Mellitus Prediction Using Ensemble Machine Learning Techniques (July 3, 2020). Available at SSRN: https://ssrn.com/abstract=3642877 or http://dx.doi.org/10.2139/ssrn.3642877

[9] Okuhara, M., Shiozaki, T. and Suzuki, T. (2010). Security Architectures for Cloud Computing. FUJITSU Science Technology Journal, 46(4), 397–402

[10] Vishal Dineshkumar Soni. (2019). IOT connected with e-learning . International Journal on Integrated Education, 2(5), 273-277. https://doi.org/10.31149/ijie.v2i5.496

[11] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

[12] Kumar, A. (2012). World of Cloud Computing & Security. International Journal of Cloud Computing and Services Science, 1(2), 53-58

[13] Sharma, S. And Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. International Journal of Innovative Research in Science, Engineering and Technology, 2(4), 994-998.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details