(IJAER) 2018, Vol. No. 16, Issue No. V, November **e-ISSN: 2231-5152, p-ISSN: 2454-1796**

# AN ANALYSIS OF THE KEY SECURITY ISSUES IN CLOUD COMPUTING APPLICATIONS

**Pavit**

## ABSTRACT

*Cloud computing also called an on-request processing model that empowers access to calculation and capacity assets on the web. In any case, purchasers are fearful about embracing this processing model since it is still tormented by security issues. Security is as yet an unsettled issue in cloud applications. In this paper, we present the key issues of information security in the distributed computing innovation and are depicted in four zones: stockpiling security, organize security, information security and virtualization. We at that point talk about certain systems for tending to the security issues. Issues identified with institutionalization, multi-occupancy, and organization have likewise been tended to for broad utilization of distributed computing innovation in different applications.*

## 1. INTRODUCTION

Distributed computing is at present the most unmistakable trendy expression in the advanced world in light of its progressive model of figuring as a utility. It gave expanded adaptability, adaptability, unwavering quality, and diminished operational and bolster costs. The speed of foundation and the simplicity of scaling up or down on request have changed the manner in which registering and correspondence administrations are utilized while improving them, quicker and cheaper1. The distributed computing model gives access to a common pool of figuring assets that the users can access through the internet2,3. Its two distinctive features include:

- the use of computation resources is under demand, and
- the dynamic and accurate assignment of computational resources are only done when they are strictly essential.

The fundamental rule of cloud computing is to transfer the computing services from the user remote computer to the network of interconnected and networked/virtualized computers4 (Figure 1). Here, it is not required to purchase and maintain the necessary resources including network, server, storage, application, service, etc.; rather, they can be used from the cloud network. One of the studies conducted by National Institute of Standards and Technology 5,6 have defined cloud computing as “computing model that enables ubiquitous, convenient, and on-demand network access to shared configurable computing resources (e.g., servers, storage, networks, applications, and services). These resources can be rapidly provisioned and released with minimal management effort or service provider interaction”7. However, many potential cloud users are reluctant to adapt to cloud computing owing to the unaddressed cloud computing security issues7,8. Inability of the owner of the data to control the placement of data is one of the key security challenges faced in cloud. With the increased usage of the Internet-

enabled mobile devices including smartphones and tablets, the amount of web-based threats also continues to rise in number thus leading to more complex situation9. Securing data is more critical in the Mobile Cloud Environment. Along these lines, it is required to viably take care of the security issues in cloud situations to empower the increasingly prevalent and safe activity of cloud everywhere throughout the industry10. As of late, numerous unique research, near examination and audit papers have been distributed that managed distributed computing security issues11,12,13. Be that as it may, enough lucidity with respect to the most appropriate issues in Cloud Computing security including the related dangers, dangers, vulnerabilities, prerequisites, and arrangements have not yet been accomplished. In addition, the security aspects associated with the virtualization in the cloud is a foundational however it's an inadequately researched area of research. This paper offers a broad discussion on the various security issues. In addition, the paper also deals with identifying, classifying, organizing and quantifying the major cloud computing security concerns and presenting the related solutions. We likewise present a scientific categorization of the security issues in distributed computing.

1.1 Service Models for Cloud Computing

NIST5 have defined the following three main service models, four deployment model in cloud14.

- Infrastructure as a Service (IaaS): In this layer, the cloud provider provides the user with both storage services as well as computing power including storage services or computation services, operating systems and the virtualization of hardware resources.
- Platform as a Service (PaaS): Here, the cloud provider provides a computing platform, tools, development environment and capability to help users build, test, and deploy web-based applications;
- Software as a Service (SaaS): Here, customer is given with a software or an application as services that can be accessed from any online device.

1.2 Cloud Computing Deployment Models Cloud computing is applied for any of the following four deployment models namely 1) private cloud 2), public cloud, 3) hybrid cloud, and 4) community cloud.

1.2.1 Private Cloud

In this deployment model, the infrastructure is operated exclusively for an organization.

1.2.2 Public Cloud

In this model, the infrastructure is owned by the organization (cloud provider), and rent the services or resources to the customers, public or a large industry group. However, this model is considered less safe and more exposed to risk compared to the other models, as its resources are located at an off-site location.

1.2.3 Hybrid Cloud

A hybrid cloud is a combination of 2 clouds.which can be a private cloud , community cloud , or public cloud18,19 and are managed by a secure network. A hybrid cloud, as a collation of

private and public clouds presents the dual benefits of each of these models thereby effectively overcoming their obstacles. This model aids in data and application portability and the infrastructure is placed at the on-premise and off-premise.

1.2.4 Community Cloud

Here the infrastructure supports a specific community and is shared by the several organizations. This cloud is controlled and shared by multiple organizations. It removes the security risks associated with the public clouds and the costs involved in the privacy

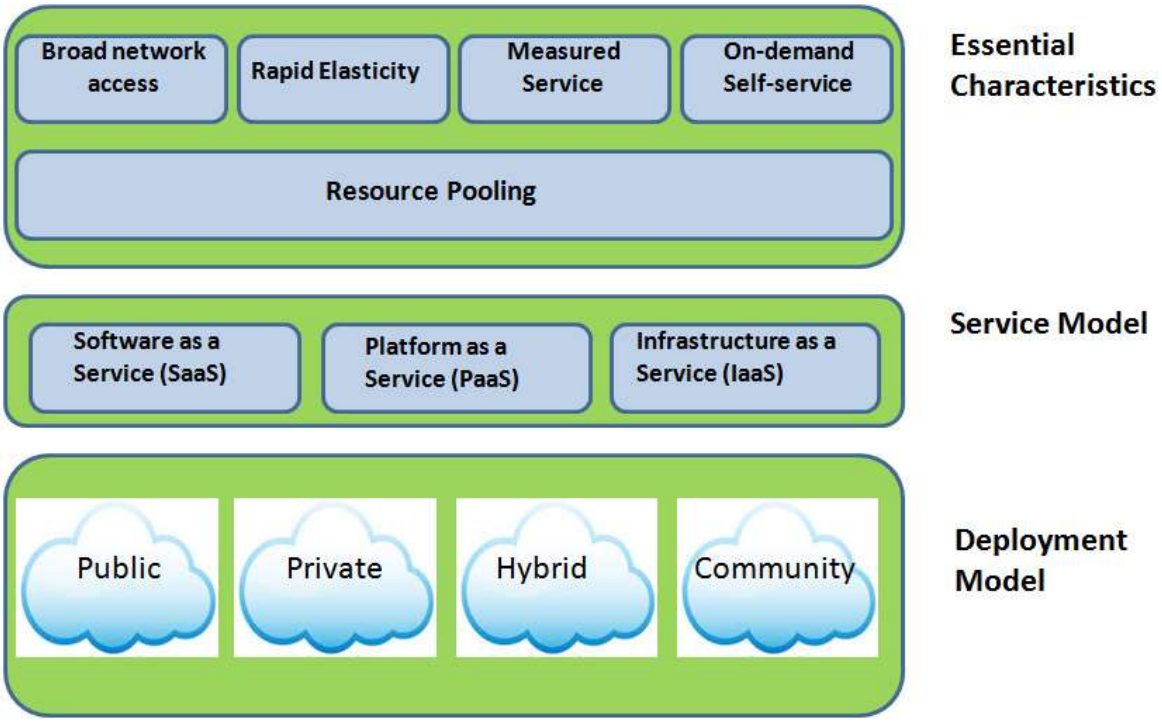


Figure 1. (a)Visual Working Definition of Cloud Computing. 31

## 2. CLOUD COMPUTING SECURITY ISSUES

Despite the benefits, there remain many open security issues because of multi-tenancy, outsourcing of application and data, and virtualization due to relocation to the clouds 20,21. The information moves outside the user's security perimeter, which increases the users' overall security risks. The IaaS model deals with providing basic security such as perimeter firewall, load balancing, etc. However, the applications that have moved into the cloud require greater levels of security provided by the host10,22. In the pass service model, the maintenance of the incorruptibility of applications and proper enforcement of proper authentication checks during data transfer across the all networking channels is fundamental22. In SaaS applications are accessed using web browsers over the internet, so web browser security is important22. A few examples of security attacks in the cloud include (i) malware injection attack, (ii) wrapping attack, and (iii) DDoS attack. With regard to deployment models, more security than public

and private clouds is seen in case of a hybrid cloud. In the case of private and public clouds, the former is more secure than the latter, which is considered as the least secure model10,22. Measuring the quality of security is difficult because the infrastructure should not be exposed. Most of the security problems in cloud computing mainly stem from three broad reasons:

• loss of control of data,
• absence of trust (mechanisms), and
• multi-tenancy architecture**.**

All the above problems usually persist in the third party management prototypes of the cloud. Apart from being associated with several privacy issues, public cloud also presents a number of security worries., According to the recent survey, security was undeniably one of the top rated challenges of the cloud model23. This section of the paper deals with the high importance problems in cloud architectures. Although the private cloud guarantees security levels to a assured extent, the costs associated with this type of approach will be relatively high. Self-management clouds may in any case have security issues, but these issues are diverse to the above reasons.

2.1 Loss of Control of Data

Clients' loss of control happens inferable from the situation of information, applications, character the executives of the clients and assets with the supplier The client legitimately relies upon the cloud supplier to ensure factors like security and protection for information and accessibility of assets.

2.2 Lack of Trust (Mechanisms)

Trusting the third party means chance of getting in to danger. Although the trust relationships might not be so stronger at any instance in the cloud delivery chain, in order to ensure quick delivery of services24. A significant risk is introduced with the adoption of a cloud service owing to the globalized nature of the cloud infrastructure and non-transparency resulting due to the loss of control in transiting the sensitive data to other organizations. Organizations that are involved in contracting outsource business processes in the cloud may not be aware that the contractors may also sub-contract these processes. In such cases, the organizations may not know the identity of the sub-contracting providers in this contracting chain. In addition, the measures for the data protection may not be known in the contract chain. Furthermore, the data protection would result in weakening of trust at all levels from the customer to the providers. The ‘on-demand’ and ‘pay-as-you-go’ model are based on delicate confidence relationship, with lax data security practices that may expose the data to third parties and makes it difficult in order to check the deletions. With the aim of providing additional capacity at a shorter period, some new providers can then be appended to the chain without adequate verification regarding their identities, praises, reputations, and trust worthiness.

2.3 Multi-Tenancy

Generally, the term Multi-tenancy refers to sharing of multiple resources and the services to execute software instances that serve multiple clients or tenants on a single machine (OWASP-10)25. The Physical resources in a cloud can be computing, networking, storage devices etc. and the services are data storage, data management, etc. are supported as well as it can be shared. The main driving force for cloud providers to have multi-tenancy is to cut down the costs by allowing the clients for sharing and reusing the resources among themselves. In this condition, security is increasingly subject to the intelligent isolation of assets than the physical partition of the assets in AVM. A portion of the security issues emerging due to multi-occupancy is as per the following. (I) Inadequate legitimate security control. This guarantees one occupant intentionally or accidentally can't meddle with the security (privacy, respectability, accessibility) of different inhabitants. (ii) Malicious or unmindful occupants: A malignant or an insensible inhabitant can decrease the security stance of other tenants if the supplier has more fragile coherent controls among the occupants. (iii) Shared services can develop into a single point of failure: If the cloud service provider has not constructed properly, they can easily develop and results in misuse or abuse by the client. (iv) misconfigurations: When the multiple clients share this fundamental infrastructure, all the changes should be formed and must be tested. (v) Combined clients Data: The CSP stores the multiple client's data in the same database, makes use of same table-spaces, and uses same backup tapes to reduce the costs. This makes the data vulnerable and can lead to data destruction, which arises a security issue in the multi-tenancy, mainly if the data is stored in shared media.(vi) Performance Risks: The excess use of the service by a single tenant may effect the quality of service. (vii) XaaS Specific Risks are provided as follows:

SaaS: The application stack may be shared by the multiple clients or tenants. This indicates that data obtained from the multiple Users may be allocated in the same database, archived or backed-up. It is then moved through the common networking devices, and will handled by the application processes. This proves mainly focuses on the logical security to isolate different clients on a single VM.

PaaS: Since the platform layer is shared between the different tenants, the vulnerabilities in this layer will results in data leakage among the clients.

IaaS: Security risks at IaaS includes cross-VM attacks and cross-network traffic listening. However, the co-residents may be faced with lower security posture 26.

## 3. RESOLVING SECURITY ISSUES IN THE CLOUD

In12 has classified the security issues into seven main categories namely: 1) network security, 2) interfaces 3) data security 4) virtualization 5) governance 6) compliance and 7) legal issues. Each of the category have several security issues, in turn classified into subcategories highlighting the fundamental security issues identified in the base references12,27 made a quantitative analysis of security aspect after analysing more than 200 references. However,

data applications may still need to be in the cloud, and the consumers may not be able to manage taking back control. The higher trust in respect of the degree of isolation is essential. Multitenancy may be minimized by adopting private cloud. Virtual private cloud (VPC) is a system, and necessitates strong separation. While the providers of VPC argue that they present utmost isolation, since the consumers' data is not residing in the separate servers and it is being stored along with the other user data. However, they are differentiated logically. In case of failure of the actual server, the consumers' files and apps stored are lost. The directly accessible confinement office inside the cloud (i.e., virtualization) isn't idiot proof and can be effectively attacked28,29,30. The issue becomes aggravated when the equivalent physical equipment has a huge number in the cloud. Therefore, the providers of cloud service should be certain about the information security on the cloud and resolve the risks to the acceptable level by using

- By using encryption scheme by which the shared storage areas protect all the data;
- By Specifying accurate access controls to avoid unauthorized access to the data; and
- Regular scheduled data backup's and storage of the backup media in secured.

This will require the establishment of information security system and trustworthiness between both the cloud providers and the universities31.

## 4. MINIMIZE LACK OF TRUST: POLICY LANGUAGE

It is a known fact that although the consumers have certain specific security needs, they do not have the authority to decide on the way they are handled. This means the consumers cannot state their requirements to the provider.

In other words, the service level agreements (SLAs) are one-sided. These SLA's generally denote the high level of policies set by the cloud provider (e.g., maintain 98 percent). In particular, the communities of interest (COI) clouds encompass separate Security Policy essentials which must be fulfilled by the cloud provider owing to nature of COIs and their utilization. These requirements should be communicated to the providers so that they can ensure that the requirements are fulfilled. Thus, the cloud consumers and providers should be presented with a standard means for stating their security requirements and capabilities. This is made possible by devising a policy language that can be used to transfer own policies and confidence, which is to be upheld by both the parties and used as an intra-cloud context to achieve the overall security aspects32. The cloud consumers need to devise a way through which they can validate the given infrastructure and maintain the security mechanisms to satisfy the requirements as stated in the consumer's policy. Consider a case, where consumer's policy necessitates the isolation of virtual machines, the CSP can devise a statement, stating that VM isolation is used for cache separation. Additional assurances to consumers can be provided in the form of highly regarded, security features, assurance and risk assessment by certified third parties.

# 5. REDUCING CLOUD LOSS

5.1 Monitoring

The failure of the underlying components should follow the determination of, its effect so that the exact recovery measures meets. An application-related Run-time Monitoring and management tool can be used32 in that situation. The applications placed in user computers, allowing user to monitor and data flow. The outputs of the primitive services are directly issued to the application logic. If any data is found incompatible among the services is posed as a problem. The capability of the run-time checking and the executives instruments should 1) guide the application client in deciding the status of the cloud assets for running the application (over numerous mists); 2) helps the clients in deciding the security issues continuously and situational mindfulness 3) empower the application client to convey the occupant information or application (or a piece of it) to the next Virtual Machine of a similar cloud or of the diverse cloud 4) make the application client fit for changing the application rationale on the fly; and 5) offer the cloud providers with communication capabilities.NimSoft and Hyperic are some cloud vendors33 provides monitoring tools which are application specific functionalities. The further enhancement of these run time Monitoring tools might be carried out or might be combination with the other tools to provide certain degree of monitoring. Somehow, it insists the tools for army purposes should also receive additional accreditation and Certificate procedures.

5.2 Utilizing different clouds

The services might be used by the consumers from the different clouds via multi-cloud architecture34, in which there are chances of increasing the risk, redundancy, as well as the chance of mission completion for several critical applications. However, the use of different clouds may lead to some particular issues such as policy incompatibility, data dependency between clouds, and knowing when to utilize the redundancy feature. Spreading the sensitive data across multiple clouds involves a lot of risk owing to the redundancy that could increase the risk of exposure.

5.3 Minimize Loss of Control: Access Control

Cloud computing has many layers in access control35. Based on the deployment model, the accesses are being controlled by the cloud provider or customer. Google Apps, is a provider and acts as a representative of SaaS cloud, In Google Apps, authentication and access policies are associated with its application and managed by the provider itself. On the other hand, client or user has the responsibility of accessing their own documents through given interface. In the IaaS type draws near, the client holds the capacity to manufacture accounts on its VM and to make the entrance control records for the administrations situated on the VM.

The CSP manages the authentication and control access process irrespective of its deployment model. Few of the providers supports federated authentication, in which the client is able to manage its users, but they are responsible for the management of access control as well.

This states that the user should have confidence on the service provider on all security related issues, data administration, and maintenance of the access control policies. This can turn out to be difficult with the involvement of the number of users from several organizations with of different access control policies. In case of the consumer managed control access, the consumer is required to keep hold of the access control decision-making process as a means of control measure. This requires investing less trust on the provider (that means Packet Data Protocol (PDP) is in consumer's side). This model necessitates the client and the provider to have standard SLA and trust relationship to describe the users, resources. It is very much necessary that the data owner should have due involvement in all requests in such approaches. Therefore, this method should be avoided if traffic is an important concern. Hence, in many secure data outsourcing process, the users are required to store keys or any certificates to the query side to involve the owner for every query to the database.

## 6. MINIMIZE MULTI-TENANCY IN THE CLOUD

### 6.1 Local Host Security

Due to the lack of security in these terminal devices, untrusted services present in the cloud may attack the local networks. The local host machines used in the present computing environment includes desktop computers, laptops and mobile devices. In general, the cloud consumers are more concerned about the cloud provider's site security. Due to this, the consumers may forget to provide security to their machines. Mobile devices have higher threats. If a user depends on mobile for accessing cloud data, this may increase the security threat as there is a possibility that the users may misplace or get their devices stolen. In addition, the potential attackers can easily enter the cloud system through handheld gadgets as the security mechanisms of tend to be insufficient as compared to the desktop computer. Features like strong authentication mechanisms, tamper-resistance, and cryptographic functionality when there is requirement of traffic confidentiality should be embedded in a device that accesses cloud data. As a portion of detaining the security depends on the consumer, the provider may be required to stipulate its policy or SLA. In case of new cloud computing approaches in mobiles, the applications are required to lie in the cloud as compared to the smart phones that enable a greater sophisticated security mechanism. Since the users use their local host machines to connect to the cloud, many of the secured cloud storing technologies ask for generating master keys (used for encrypting data, which are also known as session keys) that can be stored in the local machines used by the consumers. In consequence, if the local machine is attacked by a malicious service present in the cloud and these master keys are accessed, this causes data risk. In this case, the user's computer starts working like a zombie that can be easily accessed by the attackers to attack the stored data in the cloud. Malicious codes can be present in the computer of the user that can damage the provider-side resources, in turn affecting the provider as well as all its other consumers. Hence, developing the new technologies can be enabled the war-fighters in the use of the handheld devices for gathering data to a command centre. Hence, the major concern point rests at the robustness and durability of these devices both for cloud computing and general-purpose military use. Hence, for sensitive areas of

memories, which is the site for storing keys, the memory curtaining techniques can be used. In addition, remote attestation or "Trusted Platform Module (TPM)" type requirements may be used for ensuring security of cloud computing.

## 7.CONCLUSION

Cloud computing presents an example of the standard mainframe client-server model, with scalable, universal and availability of resources. Both the traditional and new-era threats are involved in cloud. Security has become key issue in Cloud Computing environment, data security is to be managed for current technologies and research is to be carried out. Thus, the issues involved in ensuring the cloud data security in cloud computing, such as the lack of trust, the loss of control, and multi-tenancy problems needs to be identified, to make secure and reliable for cloud computing applications. This article reviews various security techniques for protecting the data in cloud and focused in improving data security, in providing a trustworthy healthy Cloud security environment for various applications.