RESEARCH PAPER

TITLE – Cloud Computing: Security Issues And Challenges

BY

STUDENT ID:L30061878

STUDENT NAME:Siva nagi reddy peram

EMAIL ID:sivanagiperam@lewisu.edu

TABLE OF CONTENTS

ABSTRACT

Cloud Computing (CC) concept is not a new term in the present world. It has changed the business operations too much with its exceptional features or characteristics. If I talk about the term, it is originated from the diagrams exploited to symbolize the internet. Cloud computing (CC) has several benefits that may aid the business operation in several ways in gaining benefits. But, the business entity is now coming aware of several security challenges with the development of CC over time.

So, the primary task is how to deal with such issues. Such issues are also acting as a strong barrier to not opting for CC technology in the business environment by many firms. In this paper, I will present the background details of Cloud Computing (CC) as well as outline various characteristics, service, or deployment models. Here, I will also discuss several issues or challenges related to CC.

1. INTRODUCTION

1.1. Overview

CC has emerged as an innovative technology aiding firms in facilitating business operations in several ways. A user may access resources on-demand with the aid of this technology which is one of the significant characteristics of Cloud Computing (CC). If I introspect the Cloud Computing impact on the business operation, it has much changed or affected the firm tremendously.

Several big firms have already started working on the concept of CC and providing reliable, powerful, and cost-efficient cloud platforms. Organizations are reshaping their business models aiming to gain more profits from this technology. But, several issues still exist in cloud computing (CC) that need to be resolved. Security has become the key concern for the individual to shift to CC as per a recent survey done by CSA (Cloud Security Alliance).

In this paper, I will investigate the main issues of security related to Cloud Computing. In terms of the several applications as well as infrastructures, I will present the security concerns as CC refers to both the applications delivered as services over the internet as well as the infrastructures. Here are lists of security concerns that should be taken into account are as follows – Authorization, Integrity Control, Confidentiality, Availability, etc. Here are a few aspects that I will cover in this paper as follows:

- Outlining several aspects related to cloud computing covering features or characteristics.
- Reviewing various issues or challenges associated with Cloud Computing (CC).

1.2. Aim And Objectives

ASPECTS	*DESCRIPTION*
AIM	The study aims to outline the background details of CC along with the discussion of security issues as well as challenges.

OBJECTIVE	Various Objectives are: a) Presenting background details related to cloud computing. b) Discussing features, characteristics, service models, or deployment models related to cloud computing. c) Reviewing issues related to security linked with the cloud. d) Presenting various security challenges associated with the cloud.

2. CLOUD COMPUTING: DEFINITION AND CHARACTERISTICS

2.1. Overview

In this section, I will first define the term CC and then I will discuss features or characteristics of cloud computing. Service models or deployment models will also be discussed here.

2.2. Definition of Cloud Computing

Various definitions have been provided by various researchers or practitioners. Here, I am providing two main definitions which are described as follows.

Lists of Definition	***Aspects***	***Description***
1 – Definition	As per NIST	It is a model for enabling on-demand network access to a shared pool of configurable computing resources that may be released or provisioned with less human effort.
2 – Definition	As per Buyya	It is a distributed or parallel system comprising of a collection of virtualized or interconnected computers that are provisioned dynamically as well as presented as one or more unified computing resources based on service-level agreements established via negotiation between the users as well as service providers.

2.3. Characteristics of Cloud Computing

As per NIST, cloud computing (CC) carries the following key characteristics as follows:

a) *UBIQUITOUS NETWORK ACCESS* – With the aid of diverse user platforms, the resources of cloud computing may be accessed. If the manufacturing application is time-sensitive, then latency or network bandwidth can play a significant role in the case of CC.

b) *MEASURED SERVICE* – In the case of an occupant or application, the utilization of the resource is tracked. An account is provided to the resource provider or the user that can check each utilization. For several reasons, such aspects are done that include effective utilization of the resource or monitoring billing.

c) *RAPID ELASTICITY* – Offers resources that may be scaled in or out as per demand. If the requirements get over, then the resource is scaled out but provided whenever the user needs services.

d) *RESOURCE POOLING* – Cloud Computing (CC) utilizes a multi-tenant model, so the computing resources of the provider may be pooled to serve all users. As per user demand, distinct virtual or physical resources may be assigned as well as reassigned dynamically.

e) *ON-DEMAND SELF-SERVICE* – Computing capabilities may be provisioned unilaterally by a consumer – for instance – network storage or server time – as required without needing human intervention with the provider of each service.

2.4. Service Model of Cloud Computing

S. No.	*Service Model*	*Description*
	Software as a Service (SaaS)	In this case, software services are provided on-demand to the users. Here, the services need to be well-protected as users utilized software services from distinct providers. For instance – GoogleApp, Salesforce, etc.
	Platform as a Service (PaaS)	It offers a development platform to the users in CC. For instance – Google AppEngine
	Infrastructure as a Service (IaaS)	It offers the following services – for instance – storage, Network technology, servers. OpenNebula is one example of this model.

2.5. Deployment Model of Cloud Computing

S. No.	*Deployment Model*	*Description*
	Public cloud	In this case, resources are accessed quickly and need to pay only for operating resources.

	Private cloud	In this case, resources are meant only for particular organizations. Data security is the main benefit of this cloud.
	Hybrid cloud	It utilizes the combined features of the public or private cloud.
	Community cloud	This cloud is shared among several firms as well as resources are used.

3. SECURITY ISSUES ASSOCIATED WITH THE CLOUD

Now, I will make you aware of what are issues linked with CC. Several issues of security associated with CC are categorized as – (a) Security Issues Faced by Users (b) Security Issues Faced by Cloud Providers. A user needs to ensure that the provider has taken the proper measures of security in protecting their info while the provider must ensure that their infrastructure is secure as well as even the data or application of the user is protected. Here are a few lists of security issues which are described as follows.

S. No.	***Challenge***	***Description***
	Data Availability	Could the cloud merchant move their whole user's info onto an alternate climate should the current climate become compromised or inaccessible?
	Data Location	Does the cloud seller consider any command over the area of information?
	Data Segregation	Is encryption accessible at all stages, as well as were these encryption schemes planned as well as tried by experienced experts?
	Investigative Support	Does the merchant be able to research any improper or criminal behavior?
	Long-Term Viability	What befalls information if the cloud merchant leaves the business, is the customer's information returned, and in what design?
	Privileged Access	Who has specific/restricted admittance to the info? Who chooses about the recruiting and the executives of such heads?
	Recovery	What befalls information on account of a catastrophe, and does the merchant offer total reclamation, and, assuming this is the case, how long does that interaction require?
	Regulatory Compliance	Is the cloud seller able to go through outer reviews as well as security accreditations?

3.1. Security Issues Based on the Delivery and Deployment Model of Cloud

If I talk about the SaaS platform, providers are more responsible in the case of security. For security measures, users require to rely on the providers. In the public cloud, stronger security measures are needed as the public cloud is less secure than private clouds. Another important aspect that becomes hard to do in SaaS is that how to ensure that proper security is maintained or not. More extensibility may also be demanded by the private clouds for accommodating customized needs. As an integral part of the SaaS application development as well as the deployment process, the following key security aspects need to be assumed carefully as follows – Availability, Network Security, Data Confidentiality, Data Access, Data Integrity, Data Segregation, etc.

If I talk about the PaaS platform, users may develop their applications on top of the provided platforms. As providers are responsible only for isolating the workspaces or applications of the users from one another, so it is the responsibility of the users to protect their applications. Therefore, enforcing the authentication checks and maintaining applications integrity are the fundamental needs in the case of the PaaS platform.

If I talk about the IaaS platform, the main concern in it is how to maintain control over the data of the user that is stored in the hardware of the provider. The cloud provider must offer low-level capabilities of data protection. And, the users are responsible for securing the content, applications, or OS.

As the public cloud permits users to access the data across a wide area network, so it is assumed as less secure than the other cloud models based upon the deployment model. But, if a comparison is made between private and public cloud, then private is assumed more secure as it is meant for a specific organization. The figure exhibited below represents the information security needs integrating with CC delivery models as well as the deployment model. In the context of CC, each of the security needs will be outlined as follows:

S. No.	***Aspects***	***Description***
	Availability	In cloud computing, it is a significant information security need since it is the main deciding aspect when deciding delivery or deployment models. The key purpose is to ensure that the service must be available at any time or any place. This aspect is a mandatory security need for PaaS and IaaS as several vendors of CC provide cloud infrastructures as well as platforms based on VMs (Virtual Machines).
	Authorization	This aspect ensures referential integrity is maintained. Within cloud computing, it follows on privileges as well as in exerting control over process flows. If I take the instance of public cloud, several users may share resources provided by a single service provider. So, it requires proper authorization. But, authorization is maintained by the administrator in the case of the private cloud.

	Confidentiality	It is one of the significant aspects of CC. If I take an instance of public cloud, it is hard to guarantee in this case for the following reasons. • The number of growing users. • Data duplication and aggressive data caching • Non-availability of end-to-end data encryption. Thus, data confidentiality will be maximized by utilizing several private clouds managed by trusted parties.
	Identification & Authentication	The cloud service provider may have a secure infrastructure in protecting user data as well as guarding against unauthorized access as the big issues in private or public cloud incorporate compliance, privacy, data collection, or internal and external threats. Before accessing any data over the cloud, there is a need to verify or validate individual cloud users based upon their credentials.
	Integrity	Within the cloud domain, it mainly lies in applying due diligence if accessing data. So, ACID properties of the data of the cloud must be imposed without any doubt across all models of CC.
	Non-repudiation	It may be attained in cloud computing (CC) by employing the traditional e-commerce security protocols as well as token provisioning to data transmission within cloud applications – for instance – digital signatures confirmation receipts services, or timestamps.

4. SECURITY CHALLENGES

If I talk about the environments of Cloud Computing (CC), it is multinomial environments wherein each domain may utilize distinct privacy, security, as well as trust needs and employ potentially several semantics, interfaces, or mechanism. Now, I will discuss several security challenges in CC along with solutions are as follows.

4.1. Access Control and Accounting

In Cloud Computing (CC) services, the access control policy of fine-grained needs to be enforced owing to diversity or heterogeneity in it. If intends to capture access requirements (for instance – credential, attribute, or dynamically based), the services of access control need to be flexible enough. Even, relevant aspects of SLAs need to be captured by the access control models. In the case of users, records of proper accounting are needed for billing purposes as the Cloud Computing (CC) model is the pay-per-usage model. It is hard to assign roles to users directly in the case of CC as service providers do not know usually their users. So, such sort of capability may be enhanced by using attribute or credential-based policies. Several standards (for instance – Web service, XACML, or SAML) may be exploited to specify the secure access control policies.

One of the widely accepted methods among all is Role-Based Access Control owing to flexibility, simplicity, or efficient and least privilege management.

4.2. Trust Management

For various services, the user needs to depend on the provider in the cloud computing (CC) environment. But, sometimes a situation appears wherein users find a need to store the data on the side of the provider. So, a framework of trust needs to be built that may aid in capturing generic parameters set efficiently for managing or establishing evolving trust as well as sharing needs.

4.3. Data-Centric Security and Protection

Over the cloud, several users may share, access, or save the data in cloud computing (CC). In such a case, the data must be able to move from one point to another point securely and even one user must be segregated properly from that of another. So, a proper security measure must be employed by the cloud providers to prevent data leaks as well as access by 3rd unauthorized parties. Even privileges must be assigned carefully by the cloud provider to the users and also need to ensure that the assigned duties may not be defeated. Must employ policies of access control properly. A system needs to check the policies if someone intends to access data. The data security may be done by using existing techniques of cryptography.

4.4. Authentication and Identity Management

Over the internet, the user may access the info from several places by using cloud services. Thereby, a mechanism of Identity Management (IDM) is needed for users authentication that may aid in providing services based on characteristics or credentials. Such sort of mechanism must be able to protect sensitive as well as private info related to processes or users. IDM must possess by every enterprise aiming to control access to info as well as computing resources.

4.5. Service –Level Agreement

Formally, it defines the service level and describes the contract between the provider and the consumer. This aspects aids in recognizing as well as defining the needs of the user and even mitigating the conflict areas – for instance – Confidential Information Termination, Security IPR, Customer Duties, and Responsibilities, Services to be Delivered performance.

5. CONCLUSION

Here, I have discussed several security issues as well as challenges that are being faced currently in Cloud Computing (CC). Aiming to realize the benefits of Cloud Computing, more mature or newer solutions along with several enhancements in existing solutions are required urgently as the adoption of the technology is rising over time. Although the technology of cloud computing is in the early development stage, so most significant aspect that will impact its success is the security or privacy landscape, so mitigating its adoption in the business environment of the firm.

REFERENCES

1. Popović, K. and Hocenski, Ž., 2010, May. Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE.
2. Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), pp.247-255.
3. Singh, A. and Chatterjee, K., 2017. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, pp.88-115.
4. Alvi, F.A., Choudary, B.S., Jaferry, N. and Pathan, E., 2012. A review on cloud computing security issues & challenges. *iaesjournal. com*, *2*.
5. Alvi, F.A., Choudary, B.S., Jaferry, N. and Pathan, E., 2012. A review on cloud computing security issues & challenges. *iaesjournal. com*, *2*.
6. Dillon, T., Wu, C. and Chang, E., 2010, April. Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). Ieee.
7. Shahzad, A. and Hussain, M., 2013. Security issues and challenges of mobile cloud computing. *International Journal of Grid and Distributed Computing*, *6*(6), pp.37-50.