

# An Investigation into the Vulnerabilities of Cloud Computing

<sup>1</sup>Abhishek Tiwari, <sup>2</sup>Vishal Tripathi

<sup>1</sup>Research Scholar, MCA

Thakur Institute of Management Studies, Career Development & Research (TIMSCDR)  
Mumbai, India

abhitiw3147@gmail.com

<sup>2</sup>Research Scholar, MCA

Thakur Institute of Management Studies, Career Development & Research (TIMSCDR)  
Mumbai, India

tvishaly2j@gmail.com

**Abstract**—The use of cloud technology is growing rapidly in various industries, especially during the current health crisis due to the widespread implementation of remote working by companies. This shift has resulted in successful data transfer to cloud systems, enabling effortless access and manipulation on any device with appropriate authorization, rendering the necessity for data storage on specific equipment redundant.

**Keywords:** Privacy, Infrastructure, sniffing, cloud computing, service.

## I. INTRODUCTION

### A. Problem Statement:

There are various security concerns also, regarding the data integrity, software platform, privacy, and confidentiality, spanning across the vulnerability and virtualization infrastructure.

**Data integrity:** Ensuring that data is accurate and unaltered during storage, transfer, or processing. This is important because if data is modified or tampered with, it can lead to incorrect decisions or actions being taken based on that data.

**Software platform security:** Ensuring that the underlying software infrastructure is secure and free from vulnerabilities. This is important because if the software platform is compromised, it can lead to unauthorized access to sensitive information or allow attackers to take control of the system.

**Privacy and confidentiality:** Ensuring that sensitive information is kept secure and protected from unauthorized access. This is important because if sensitive information is accessed by unauthorized parties, it can lead to financial losses, reputational damage, or other harm.

**Vulnerability:** Ensuring that the virtualization infrastructure is free from vulnerabilities. This is important because if vulnerabilities are present, they can be exploited by attackers to gain access to the system or steal sensitive information.

**Virtualization infrastructure:** Ensuring that the infrastructure supporting virtualization is secure. This is important because if the infrastructure is compromised, it can lead to disruptions in service or unauthorized access to sensitive information.

Overall, the statement is highlighting the importance of considering various security concerns when utilizing virtualization technology to ensure the safe and secure operation of the systems and applications that rely on it. Ensuring security in the virtualized environment requires a holistic approach that covers all the components of



the infrastructure and software stack.

*B. Objective and Scope:*

The main objective is to adapt the data security and privacy as it is very important to maintain the privacy of the data along with the data integrity. As we know various mechanisms and algorithms are also implemented for the above issue.

*C. Process Description:*

In the initial phase of these entire pandemic due Covid- 19, we have seen that through various ways the data is lagged through various ways. That may include the hardware to copy the data or else the software scanning So, here we are trying to cover the prevention measures and finding different ways so that we can stop to leak the data.

*D. Purposed Solution:*

To Find the solution by finding all the different ways to avoid the spamming or sniffing into other user's data.

## II. MAIN REPORT

*A. Objective of the project:*

The actual definition of the cloud computing is, It is a service oriented application and not application oriented.

As we know right from the MNC to small scale companies all use these service-oriented applications. So are major focus to put a barrier to the persons who try to misuse these services and leak the data for their personal benefits.

*B. Scope of the project:*

The utilization of cloud computing services is prevalent across various industries and sectors, including the delivery of goods and services through the internet on demand, such as e-commerce platforms like Swiggy and Myntra. Infrastructure hosting over internet (E.g. hosting Servers to store data virtually).Provides Elastic Services (E.g.: Amazon Elastic Services).Hosting application services (E.g. Salesforce) Holding Next Generation Data for Various Research and Development.

As we can use these services in different areas, we do have a long list of its benefits while working on these service- oriented applications.

1. Shared Infrastructure: Which means any company which uses these services will create its virtual infrastructure on the internet, and if you are part of that infrastructure as an employee or a student, you can easily access and utilize the data stored within it. This shared infrastructure model allows companies to save costs on hardware and maintenance, and also allows authorized users to access and collaborate on data from any location, as long as they have internet access. This flexibility and scalability of the shared infrastructure makes it a popular choice among companies of all sizes and industries. Additionally, this model of shared infrastructure also allows for easy data backup and recovery in case of any unforeseen incidents.

2. Network Access: This means user can access the resources from any corner of the world, just he require the proper Internet connection for his device (E.g. Mobile, laptops, Desktops, tabs etc.)

Dynamic Provision of Data: This is one of the main reasons why major companies have adopted these services. Most of them have very crucial data which just cannot be deleted or ignored as it contains decades of information. This data is critical for the company's operations, research and development, and decision-making. The ability to store and access this data from anywhere in the world and at any time is a key benefit of cloud computing services. Additionally, the shared infrastructure model allows for easy collaboration and data sharing among employees, partners, and other authorized users, which is essential for companies that operate globally. By utilizing cloud computing services, companies can also save on costs associated with maintaining and



---

upgrading physical servers, data storage and backup, and IT staff. This allows companies to redirect their resources to other strategic areas of their business, making them more competitive and efficient.

So over here the user can upload millions of records just not to worry about the storage. Best e.g. over here is the social media like Facebook, Instagram, over here millions of public are uploading various videos and pictures and still is secured in the servers which are virtually created in clouds.

*C. Theoretical Background:*

Let's now have an inside look of cloud services. Till now we have just analysed the advantages and disadvantages of it but now we may cover the actual mechanism of cloud services. Basically, these cloud services are divided into three major sections:

1. Software as a Services majorly known as SaaS
2. Platform as a Service majorly Known as PaaS
3. Infrastructure as a Service majorly known as IaaS

*SaaS:* Over here all the services are provided to the host and then clients can use all the services. These services are loaded on a central storage server in short we can say entire software is created with all the requirements of the clients and then rented to them.

*PaaS:* In this case, the word itself suggests that it creates a basic platform for the client where , the client himself can create services as per his norms and condition .For eg Microsoft Window Azure and Google App engine .

*IaaS:* As the word suggest, it creates the cloud infrastructure for the clients and open that the client creates its application or any services whichever format he wants. E.g. Salesforce CRM creates such kind of infrastructure.

*D. Applications of Domain:*

Cloud services are used by a wide range of companies and organizations, including small businesses and large multinational corporations. Some examples of specific applications of cloud services include: Virtual Desktop Infrastructure (VDI), which allows users to access and work on a remote desktop using valid credentials. This is used by companies like Dell, Accenture, and TCS. IBM's Cloud Pak Solution, which integrates data across cloud and on-premises systems, and includes features like security, automation, and multi-cloud management. Softchoice, which provides services like cloud workload assessments, cloud workloads, and 24/7/365 managed services to their clients, Phoenix nap Cloud, which focuses on providing data security and compliance for their clients. Amazon Web Services (AWS), which is a popular platform for hosting static websites and applications and is known for its security and reliability. Microsoft Azure, which is used to create and support various operating systems and applications.

*E. Moving to the cloud results in a 84% decrease in carbon emissions:*

According to Accenture, companies that consistently prioritize environmental, social, and governance (ESG) factors tend to have 4.7 times higher operating profit margins compared to those that do not prioritize ESG. Using Infrastructure-as-a-Service (IaaS) can help environmentally conscious companies decrease their carbon emissions by 84% and decrease energy use by 64%.

Accenture created a chart that illustrates the difference in carbon emissions between cloud-based and on-premises operations.





Fig. 1. Cloud reduces carbon emissions.

### III. SURVEY ON LITERATURE

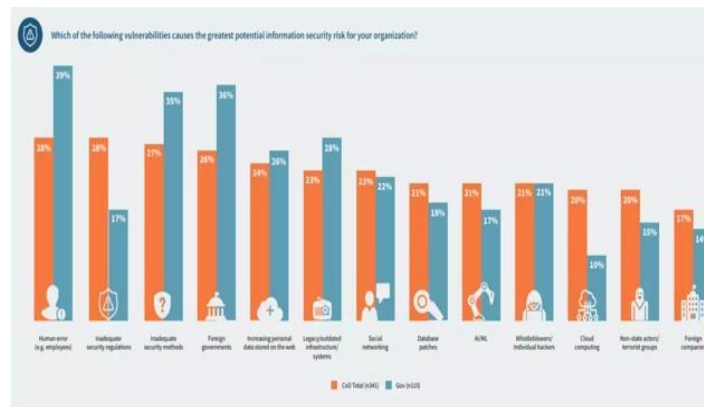


Fig. 2. Potential information security risk for organization.

In this paper, we survey the most common security concerns of current Cloud Computing systems. Cloud Computing refers to the delivery of applications and services over the Internet. Some of the questions frequently raised by the public include:

1. What happens to my data when it uploaded to the cloud?
2. Is my data secure when it is stored on cloud servers?
3. Can third parties access my data without my permission?
4. Who is responsible for securing my data on the cloud servers?

One of the authors of the paper has provided the following answer to these concerns: when a person uploads data to the cloud, it is converted to a specific format and then stored on specific servers. Once the data is on the server, it is compressed into a format that can only be accessed by answering a set of security questions, such as date of birth or hobbies. This is done to ensure that only authorized users can access the data and to protect it from unauthorized access.

The application that you are using will determine whether your data can be accessed by third parties.

If the application does not allow for third-party analysis, then your data will remain private. According to Quora, there are various types of clouds available and the choice of which one to use depends on the needs of the client. Community clouds allow multiple customers to access data, but all users are authenticated. Regardless of the type of cloud, they are all safe and secured.



---

#### IV. RESEARCH AND ANALYSIS DESIGN

In simple terms, Cloud computing is a new way

of using technology where multiple computers work together to perform tasks. There are three main types of services offered: SaaS, PaaS and IaaS. SaaS companies offer software applications, PaaS companies offer the platform for creating applications and IaaS companies offer the necessary infrastructure for applications. Different companies like Google App Engine and Amazon Elastic Services provide these services. However, the most difficult aspect of Cloud computing is keeping data safe and secure.

The reason for the lack of security in data on cloud services was that the initial standards of the services or products were not met. However, standards have been raised by the Cloud Security Alliance (CSA), leading to a decrease in attacks.

##### A. Security Frameworks:

A framework was introduced to address security concerns in cloud computing. One of the key components of this framework is the use of firewalls. Firewalls in cloud computing provide an additional layer of security by limiting access to specific ports. For example, the web server port number is typically 80 (for HTTP), the application server port number is typically 8000, and the MySQL server port number is typically 3306. This helps to prevent unauthorized access to the system.

##### B. Security Measures for IaaS, PaaS and SaaS are as follows :

In Software as a Service (SaaS), username and password authentication is used to prevent attacks. Additionally, advanced features such as password changes, one-time passwords, and options for fixed or long length passwords can be enabled to further secure the application. In Platform as a Service (PaaS), to prevent attacks, user activities can be restricted and special permissions from higher authorities are required to perform certain operations. In Infrastructure as a Service (IaaS), to secure the infrastructure provided to clients, it is important to separate local data backups from main server backups, and to take periodic backups to ensure that data can be recovered in case of hardware failure.

#### References

- [1] [https://www.researchgate.net/publication/309321387\\_Data\\_Security\\_in\\_Cloud\\_Computing](https://www.researchgate.net/publication/309321387_Data_Security_in_Cloud_Computing)
- [2] <https://www.softwaretestinghelp.com/cloud-computing-service-providers/>
- [3] <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/>
- [4] <http://www.e2matrix.com/blog/2018/05/21/current-research-topics-in-cloud-computing-security>
- [5] [https://www.researchgate.net/publication/220985670\\_Cloud\\_Computing\\_Security-Trends\\_and\\_Research\\_Directions](https://www.researchgate.net/publication/220985670_Cloud_Computing_Security-Trends_and_Research_Directions)
- [6] [https://www.delltechnologies.com/en-in/cloud/dell-technologies-cloud.htm?gacd=9688261-7004761040-2717743400&dgc=ST&gclsrc=aw.ds&ds\\_rl=1287495&&gclid=CjwKCAiApNSABhAIEiwANuR9YJ\\_HtXrVr0BrimmPyFYVYiA9ewr6OYba2TFTS1kOFFifoBBWLazrxoCdeIQAvD\\_BwE](https://www.delltechnologies.com/en-in/cloud/dell-technologies-cloud.htm?gacd=9688261-7004761040-2717743400&dgc=ST&gclsrc=aw.ds&ds_rl=1287495&&gclid=CjwKCAiApNSABhAIEiwANuR9YJ_HtXrVr0BrimmPyFYVYiA9ewr6OYba2TFTS1kOFFifoBBWLazrxoCdeIQAvD_BwE)
- [7] <https://www.cloudzero.com/blog/cloud-computing-statistics>

