# CLOUD COMPUTING SECURITY ISSUES

**Team: Project Team 11**

**Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson**

# Table of Contents

## 1. Executive Summary

The initiative of this project is to provide a deep understanding of what cloud computing actually is, a basic understanding of how it could be used across the organizations, and the security issues it presents. This project will focus on the security issues promulgated using cloud computing. There is a complete manifestation of 10 security issues initiated with the use of cloud computing. The approach of the project is general, but issues raised are specific. The reasons behind the issues and the vulnerabilities of cloud computing are focused. As, we know that all the technologies could be vulnerable for individuals/professionals these days. Theories and figures related to the security issues of would also be discussed. Nonetheless, the advantages and usage of cloud computing would also be kept forth as every technology has both positive and negative spectrum. The security issues are infinite as no one can focus on each aspect, but the usability of cloud computing is more than that of its vulnerabilities. All the information taken from journal articles, IEEE articles (though, self-described) will be cited properly and the main theme of the project 'Security issues of Cloud-Computing would be described' in all aspects. At the end, the conclusion of the whole report will be kept forth that what we have described related to security issues of cloud-computing. The issues would be clearly documented.

## 2. What is Cloud Computing?

### 2.1 Definitions:

**Cloud Computing:** "the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer." (Google, definition)

The Cloud is the best place to store your data nowadays. For example, if your work documents are stored on your home desktop, but you need to access them on your work laptop; they can be accessed remotely from any one of your devices. Location is not a problem for the cloud, if you are connected to a cloud server you can access anything that you have

stored on it. This is made possible because the cloud uses consolidated gadgets and applications like data accumulating, server administrators or so called (databases), frameworks organization (D.B.M.S).

The Cloud is endless and, so there is no limit to the number of documents that can be stored in it. You will never run out of space if you use the cloud. Content can be compiled on a hard drive or any data-accumulating device, this limit by cloud providers, which makes it possible for individuals to save documents to a system or a database.

This is the reason why companies have made large investments into cloud computing software. Some people that use the cloud today are sometimes unaware that they are using it because it is so versatile. “Cloud computing can provide services via the network to a wide range of customers, who, in many cases, are even unaware that they use clouds. Cloud computing combines many current technologies with each other or even combines them with new ones to achieve a new level of quality.” (Chodorek, 2014)

## 3. Introduction to Cloud Computing Security:

Intellectual property (IP) can be stored on a cloud-based server, which can host online platforms. This platform will act as an access point for users to access the cloud and for cloud providers to monitor and protect said intellectual property. Here are a few examples of content that can be stored on the cloud: personal information, company policies, organization share hubs. These are just a few of things that the cloud can store and protect. If it can be stored on the cloud it can be protected on the cloud. Service providers have put in applications that will protect the users: firewall, two factor authentication, and access controls just to name a few techniques. There are three types of cloud; these clouds store the information specified above. Cloud providers can customize their security plans based on the type of data that they are protecting.

**Private or Personal Cloud:** The private or personal cloud is a cloud that stores the personal information of an individual. Here are some examples of what can be stored and protected on the cloud: financial information, client information, digital assets, and sensitive information.

Several access controls are put in place to protect this data. Users have trusted their information with the cloud providers so the least that they can do is keep it safe. Users store their information on the cloud so that they can access it from anywhere on any device. Some examples of highly security clouds are Amazon, Google, and Microsoft. We cannot cover every provider of the cloud, but we can give a general statement that sums up the similarities that they have. They all follow cyber-security laws and regulations, so that they operate within boundaries that dictate what they can and cannot do. Highly secure digital environments are trusted by users because of their reputation of following the laws and regulations. This is the reason why users so readily trust their digital assets with these cloud service providers.

**Open or Organizational Cloud:** Cloud service providers also provide cloud systems that offer additional services other than protecting and storing. Virtual sharing platforms are constructed to store company's intellectual property and to share said intellectual property with users that are a part of the company. The organizational cloud is used by educational institutions and organizations. An organizational cloud is an open environment where the users can store and simultaneously share the information with designated individuals. The more sensitive information stored on the web the more likely users' information will be targeted. All data stored on the cloud has the potential of being stolen, this potential can be reduced if cloud providers implement the appropriate security measures.

**(Hybrid) Cloud:** The features of both private and open cloud are present in the hybrid cloud. Users can access the cloud privately or publicly. Higher security features are put in place because of the hybrid cloud's ability to be manipulated in accordance to the cloud providers preferences. The Hybrid cloud is more effective and efficient than the Private and Open Cloud. On the off chance that the user uses an automatic or also known as a hybrid cloud, the cloud can be controlled as an inward system administrator (DBMS); the features of the open cloud can be used when the cloud provider specifies it. (project, 2015) There may be times where information and applications should be moved from the private cloud to the open cloud. Here are some examples where moving the content is unavoidable: planned support, power outages, and catastrophic events. The hybrid cloud has the capacity to flawlessly relocate data, and this

is ideal for clouds recuperation arrangements and forestalling information misfortune. (Woodford, 2018)

Ecommerce businesses operate online, their entire company is stored online, from their office, customer data, customer interactions, and trade secrets. Ecommerce businesses have been working like this for a long time. Some would contend that Ecommerce can compete with the services that cloud providers specialize in.

## 3.1 Cloud Computing Services

**Infrastructure as a Service (IaaS)**: "This is where pre-configured hardware is provided via a virtualized interface or hypervisor. There is no high-level infrastructure software provided such as an operating system, this must be provided by the buyer embedded with their own virtual applications." (Tarzey, 2010) This can be described as the most basic level of cloud computing. It is a pre-configured hardware that can be purchased and adjusted by the buyer upon delivery. This service will be used if the company does not plan to outsource and will perform all cloud computing activities in house. This can be described as "in house" security, everything is controlled by the company. They can store, provide and protect their own data and the platform that stores the data. The have full control of what authorization and authentication factor are put in place. It is not recommended to perform "in house" security when the company is small. The company will lack the resources necessary to maintain and protect their assets. Companies that that jump headfirst into cloud computing and fail to look before they leap will be marked as easy targets for hackers.

**Platform as a Service (PaaS)**: "goes a step further and includes the operating environment including the operating system and application services. PaaS suits organizations that are committed to a given development environment for a given application but like the idea of someone else maintaining the deployment platform for them." (Tarzey, 2010) This is more advanced than IaaS as the operating system is included. The company will have some control of the cloud, but a secondary party will be managing the platform where documents are stored. This relievers developers of the task of maintaining and protecting an online platform, because

another party is taking care of it. The security of this platform can be described as two party's working together with the same goal. The company has the hardware and controls their own servers, and the cloud provider provides an interface where data can be stored. The cloud provider is protecting the platform while the company maintains the servers. The data stays with the company, but the tools are provided to help the company store their data

**Software as a Service (SaaS):** "offers fully functional applications on-demand to provide specific services such as email management, CRM, ERP, web conferencing and an increasingly wide range of other applications."(Tarzey, 2010) This service allows for companies to host everything online. No hardware needs to be bought; the only thing that needs to be bought is the software. The company will enlist the services of cloud providers. They will maintain the servers and host the online platform. This option is for companies that do not have enough resources and personnel or are unsure where to start, when implementing the cloud into their workplace. The security on these platforms have various methods of authentication put in place. SaaS platforms must have at least two factor authentications to keep the contents of the cloud safe. Data is given to the cloud provider and they are protecting things that they were asked to take care of.

## 4. Top 10 advantages of Cloud Computing Security:


figure 1(Eshna, 2013)

The following is a list of advantages provided by Eshna:

**No Maintenance**

Hardware will need maintenance in its lifetime. Machines are bound to break down and stop working eventually. Software does not have this problem. Cloud computing services are hosted online. They are connected to cloud servers and servers need to be maintained, but that is the job of the cloud provider. The user will never have to perform maintenance.

**Reliable**

Cloud providers have a reliable number of servers at their disposal. This is their way of managing the risk of an outage. If one server goes out, there is more than one to take its place.

**Very Secure**

In the right hands cloud computing has the potential to be very secure. If the right access controls are put in place online platforms can be an impenetrable fortress. Concurrently if lackluster controls are put in place; the door will be open to malicious attacks.

**Flexible**

The cloud can be accessed from any location at any time. If you have a tight schedule and you are not able to make it to work on time, you can access your work document at home or on the go. Workers that use the cloud have a relaxed schedule compared to those that do not.

**Cost-effective**

Cloud-computing is cost effective, because cloud providers offer deals that do not require users to purchase the whole package. Users can buy what they need; if they need a specific software program, they can purchase it without any extra attachments. Small companies can also purchase additional services when their company expands. Cloud providers can provide services to a diverse market.

**Easy Backup and Recovery**

Data saved in the cloud is not stored on a hard drive. Data is stored on a cloud-based server. Since everything is stored on a server the data has little risk of being lost. If data is lost it is easy to recover it and back it up. Apple has cloud services installed in all their devices. You can log into your iCloud account on a new phone, and your data will reboot to its last save.

**Quick to set up and convenient to integrate**

Set up is quick and easy; simply purchase the software from the cloud provider and download the software after purchasing it. Additional purchases can be made to expand by adding more accounts to your online platform.

**Huge amount of storage and capacity**

Cloud providers offer unlimited storage of data. If you purchase these plans you will never run out of data. If you purchase a limited data plan, you will run out of data, but more data can be purchased for a small fee.

**Improves competitiveness**

Small businesses, who do not have the resources to host their own server and online platform, are able to compete with large companies. Small companies are at a huge disadvantage when considering the technological work environment maintenance costs that businesses face today. Small businesses can save money by purchasing SaaS, offered by a third-party company. This will give them a fighting chance when they are competing with larger companies that have more resources and personnel.

**Environmental Benefits**

"Cloud computing reduces hardware consumption, carbon dioxide emissions and energy costs. At any given time, servers are used as per requirement and this saves a lot of energy." (Eshna, 2013) The carbon footprint is reduced because there are less hardware devices circulating in the environment, because cloud computing is hosted on cloud-based servers.

## 5. Security Issues of Cloud Computing

To sum up the major security issues of cloud computing, we can conclude that all major aspects via the use of security is hindered via using cloud computing, we have completely ascribed how cloud computing is initiated. But, as per the actual topic, it would be extensive using all security vulnerabilities of cloud computing. As per overlooking all the possible endeavors. (Morrow, March 5, 2018) (Utley, 2018) (AI, 2017)

### 5.1 System Powerlessness (Vulnerabilities):

The main and most critical issue when using cloud computing are the vulnerabilities. Though, the count of vulnerabilities of the system is infinite but somehow, we can conclude the major ones. Cloud (Remote) systems might contain structure security issues or most probably system security issues, particularly in systems that have complex foundations and different outsider stages. When any vulnerabilities have a renowned untouchable structure, the shortcoming might be conveniently used against affiliations. Appropriate fixing and overhaul conventions notwithstanding system checking arrangements are basic for battling this danger. Distributed (cloud) computing security issues are not outlandish; truth be told, a considerable

number of the dangers above can be ensured against using a devoted information assurance administration. The information in cloud insurance arrangements will both shield information from misfortune and against digital security dangers, allowing organizations to use the influence of the cloud without the related hazard. Suitable maintenance or up-gradation shows despite framework overlooking issues meant to be essential in combating the attack situation on Cloud. The security issues of cloud do not seem as dangerous as they look; the critical count of the issues occurring above can be guaranteed when using a committed data confirmation code. The data in cloud protection system would both shield data from adversity and against computerized digital attacks, allowing associations/organizations to use the impact caused by cloud as per not knowing the actual danger (Husnain, 2020)

## 5.2 Inadequate Investigation/Determination Increases Cyber-Security Risks

New companies moving to the cloud produce inaccurate determinations about the cloud and bite off more than they can chew. Professionals can send and store digital assets on a cloud-based server, but if they are unaware of the potential risk that the cloud has in store for new businesses, they should reconsider their ambitions. New business and especially small business will be targeted by hackers because of their lack of security resources. They should employ the services of cloud solution providers because they have resources and they know what they are doing.

## 5.3 Unexpected Erasure of Sensitive Information:

Data from the cloud needs to be kept secure. If a user's data stored on the cloud is attacked by hackers, everything connected to a single user's account will be jeopardized. When an account is hacked using SQL injection, password hacking, or cyber activism. Three aspects of the data are at risk the confidentiality, integrity, and availability of the data. The loss of these features will be detrimental to the organization.

## 5.4 Loss of Confidentiality of Data:

The potential loss of assets on the cloud can be described as a loss of confidentiality. Losing the confidentiality of the data is a huge loss, as the data could be handed over to cyber terrorists who specialize in stealing information from the cloud. Stolen data will more than likely be circulated on the web and competitors will have access to trade secrets. The data will no longer be confidential, because once it is leaked it becomes common knowledge. Everything that was connected to the hacked account is also compromised.

## 5.5 Loss of Integrity of Data:

Sensitive data being leaked on the web can be described as a loss of integrity. The data can be spread to competing companies. The reliability of this data will be reduced to zero and the document associated to it will need to be terminated. The leaked information can get tampered with. When data is tampered with it starts becoming unreliable; no one will believe that this data is accurate.

## 5.6 Loss of Availability of Data:

When data is stolen it can be described as a loss of availability. The data is no longer readily available for employees who frequent the cloud. The data that was stolen cannot be recovered, or it compromised and requires termination. This data cannot be recovered and is lost forever, because of a small leak anyone trying to access the document has been denied.

## 5.7 Social Engineering Attacks

Social engineering or better known as phishing can be described as, using sociological tactics that will entice someone to give away their personal information. After the information is disclosed the information will be sold to the highest bidder. The cloud is protected by a series of firewalls and access controls, but social engineering tactics can break down all the security defenses put in place. They can access the users cloud account because they have already stolen one of the keys. The user has let their guard down and either trusts the phisher or

believes in what they have promised. This is dangerous and having a false sense of security, will compromise everything that the user holds dear. There are many methods the phishers use and most of their methods will go unnoticed and will only be revealed after their goals have been achieved. Phishers are meticulous, because once they spot their target, they will watch them and wait for their chance to attack.

### 5.8 Authorization and Authentication Concerns:

If the cloud is not secure and proper authorization and authentication tactics are not set in place. The data stored on the cloud will be leaked. Issues arise when proper authentication strategies are not put in place. If little to no password protection recommendations are put in place the cloud can be broken into. Having a single password or no password at all is like leaving the front door open; nothing is stopping anyone from walking through that door. Cloud platforms that are protecting sensitive information need to have at least two factors of authentication if they want to be considered as a secure environment worthy of users' trust.

### 5.9 Unintentional Sharing

Data stored on the cloud can be shared to anyone, but users should be careful when considering who they should share their data with. Cloud providers need to have access control options that allow the user limit alterations of shared content. Cloud computing administrations give an assortment controls read only and removing download capabilities just to make a few.

### 5.10 Client Information Loss and Financial Data Issues:

Organizations store company and client information on the cloud, and hackers who have ill intent will want to steal client payment information. Companies trust cloud providers with their information, but if the correct access controls are not put in place data can be stolen and trust will cease to exist.

## 6. Figure showing Security issues of Cloud Computing

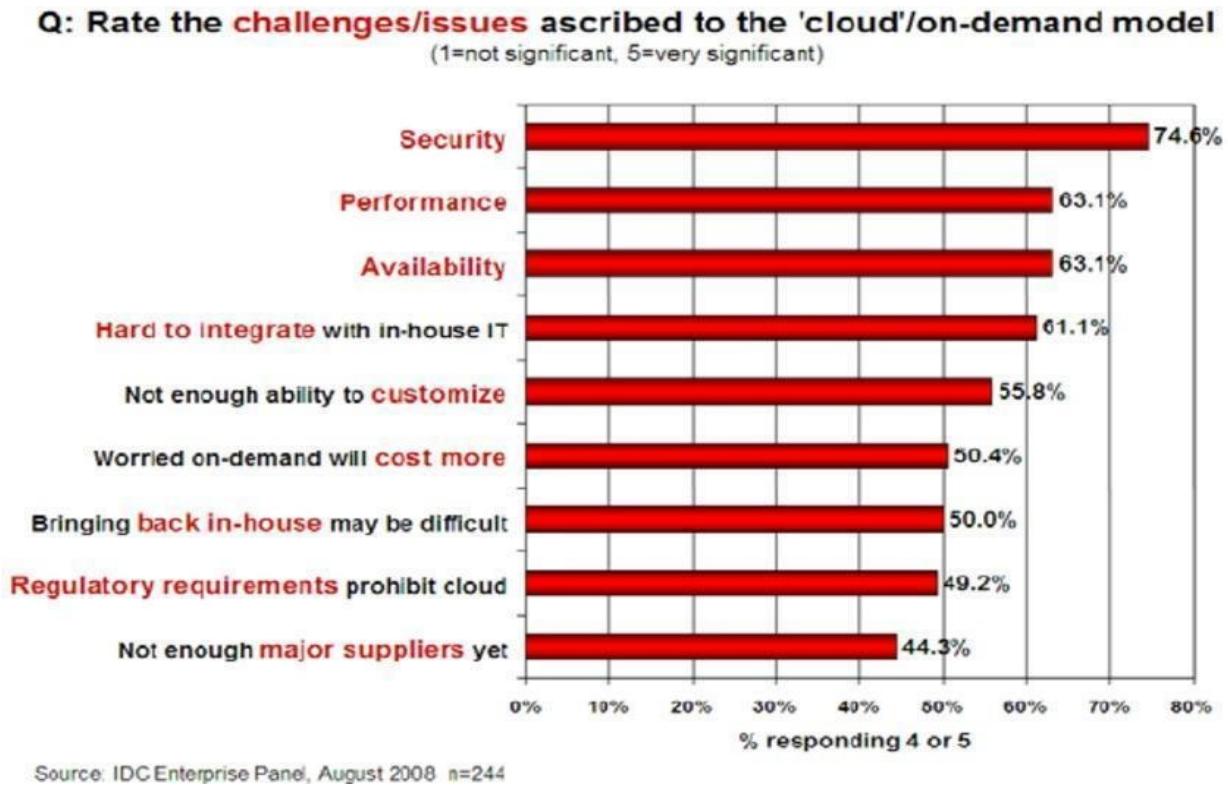


figure 2 (INFO, IDC; 2008)

This graph displays the most significant issues that cloud computing faces. The most significant issue being security was rated at 4 or 5 (5 being the most significant) by 74.6% of those surveyed.

## 7. Conclusion:

In conclusion we have defined cloud computing “as the use of remote network servers to store, manage, and process data instead of a local server or personal computer.” The main benefits of cloud computing determined in our report include: increased agility (easy access to a range of technologies increasing ability to innovate and use resources as you need them), elasticity (the ability to scale resources in order to match the capacity of your business needs), cost savings (due to economies of scale the variable expenses of cloud services are often cheaper than implementing your own IT), and the ability to deploy globally at a rapid pace (due to remote access and distributed infrastructure, applications can be expanded to new geographical

locations reducing latency). Key disadvantages of cloud technology are focused on increased information security risks. These risks are primarily generated by common cyber security threats, such as DDoS attacks, employee negligence, data loss from inadequate data backups, phishing and social engineering attacks, and system vulnerabilities. We have also compared the pros and cons of cloud computing. While using cloud computing offers increased accessibility, this results in increased vulnerability. An organization must consider the costs and benefits before implementing an Infrastructure, Platform or Software as a Service. Many organizations may be able to cut IT costs by using a 3rd party cloud service provider, large corporations handling substantial amounts of data may find it more cost effective on a long term basis to implement their own cloud service despite higher upfront costs of implementation. Organizations thinking about using cloud technology must fully consider the associated risks to mitigate them and defend their information.

## Works Cited


AI. "Cloud Computing Research." Proposed analysis (2017)

Chodorek, Robert. “Book Review.” IEEE Communications Magazine, vol. 52, no. 3, Mar. 2014, p. 11. EBSCOhost, doi:10.1109/MCOM.2014.6766073.

Eshna. (2013, February 19). Top Ten Benefits of Cloud Computing Security Training from https://www.simplilearn.com/cloud-computing-security-training-benefits-rar412-article

Husnain, Ali. "Cloud Computing - System Vulnerabilities." Cloud Computing (2020)

INFO, IDC. "CLOUD SECURITY ISSUES." CLOUD SECURITY ISSUES (2008)

Morrow, Timothy. "Risk, Threats, Vulnerabilities in Cloud." Risk, Threats, Vulnerabilities in Cloud (March 5, 2018)

Project, Enterprisers. "Private, open and hybrid cloud." Private, open and hybrid cloud (2015)

Tarzey, Bob (07 June 2010). The Computer Weekly guide to Cloud Computing. Retrieved July 01, 2020, from

https://www.computerweekly.com/photostory/2240109268/The-Computer-Weekly-guide-to-Cloud-Computing/2/The-difference-between-Saas-Paas-and-Iaas

Utley, Gary. "6 common cloud issues." cloud issues (2018)

Woodford, Chris. "Cloud Computing." Cloud Computing (2018)