CLOUD COMPUTING SECURITY ISSUES

Team: Project Team 11

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

1. Table of Contents

1. Executive Summary

In order to sum up the summary of this project. The main and basic initiative of this project is to provide deep understanding about what actually is cloud computing – its definition, basic understanding of how it could be used across the organizations. The main idea of this project is actually the security issues promulgated by the use of cloud computing. There is actually 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 reason behind the issues and the vulnerabilities of cloud computing are focused as a whole. 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 and every 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 possible 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, as long as 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 amount 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, the 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 in a remote system of cloud is actually ought to be in the cloud it viable to provide users and it also could be any usable or so forth any virtual space within a cloud. Cloud Solution Providers which actually provide cloud service do indulge client's customers to store records and applications on remote servers and a while later to get all the data through the Internet. It infers the clients or end-users of cloud which has not required to include a specific imitative to make it, allowing the end user to conclude the daily tasks via the use of remote system in the cloud

There are actually known to be as the three types of the cloud and the security issues are variably divided into these clouds

There are basically three types of clouds, which makes its usability worth able and security issues also occur with respect to its Private or Personal Cloud: The private or personal cloud is a cloud which has personal information of any person, one can store his financial information, client information, digital assets or any sensitive information as there is chance of getting hacked, as we all know that it provides encryption. Anyone uses these cloud systems in order to get higher security viability. High security clouds such as amazon, google and Microsoft. Though, we can sum up all of them to provide a generalized approach that all of them follow the cyber-security laws and regulations. One can highly secure his digital asset inside the personal cloud as it provides virtual space by and from in order to store the data of users in the additional space provided by the cloud.

Open or Organizational Cloud: The CSP's also provide such Cloud systems which provide additional virtual remote space for all organizations. It is open and data security is provided but at organizational level. There are many chances of data available at the organizational level to be hacked because it might get into social engineering attacks and employees. Open Cloud should be used in educational institutions, organizations or gatherings.

A mixture of private and open cloud (Hybrid) cloud: The features of both private and open cloud are used in the hybrid cloud systems. It could also be private or either in public. One can use this cloud at both edges. Either privately or either publicly. It includes high security features. It is more effective and efficient than that of Private and Open Cloud. On the off chance that you are utilizing an automatic or so recognized as hybrid cloud, you can control an inward system administrator (DBMS) and utilize the open cloud when required. (project, 2015) There may be times when you should move information and applications from the private cloud to the open cloud, for example, planned support, power outages, and catastrophic events. The capacity to flawlessly relocate data is ideal for cloud fiasco recuperation arrangements and forestalling information misfortune.(Woodford, 2018). (project, 2015) All we can do is to store information on or run programs from the hard drive that is called nearby capacity and registering.

All that you need is truly near you, which means getting to your information is quick and simple, for that one P.C, or others in the neighborhood arrange. Working off your hard drive is the manner by which the P.C business worked for quite a long time; some would contend it's as yet better than distributed (cloud) computing.

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 preconfigured hardware that can be purchased and adjusted by the buyer upon delivery. This service will be used if the company doesn't plan to outsource and will perform all cloud computing activities in house.

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.

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.

4. Top 10 advantages of Cloud Computing Security:

figure 1(Eshna, 2013)

No maintenance

Hardware will most likely need maintenance in its lifetime. Machines are bound to break down and stop working sooner or later. 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 amount 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 don't.

Cost-effective

Cloud-computing is cost effective, because cloud providers offer deals that don't 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 are able to 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 of 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

In order 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 extensively using all security vulnerabilities so and forth via the use of cloud computing. As per overlooking all the possible endeavors. (Morrow, March 5, 2018) (Utley, 2018) (AI, 2017)

5.1 System Powerlessness (Vulnerabilities):

The first and foremost issue which damages cloud computing is vulnerabilities. Though, the count of vulnerabilities of the system is infinite but somehow, I'll 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 significant 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, permitting 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 seem as not dangerous as actually they seem like; the critical count of the issues occurring above can be guaranteed as utilizing 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 in order to utilize the impact caused by cloud as per not knowing the actual danger (Husnain, 2020)

5.2 Inadequate Investigation/determination Increases Cyber-Security risks

Companies moving to the cloud frequently perform inadequate determination/investigation. Professionals can transmit or store the digital assets of a professional on a Remote Cloud System as they don't know what could happen if the data saved in the cloud gets hindered or gets affected in any way. Cloud Software/Solution Providers should only focus on providing the end-users with high security rather than investing about the system need. The End-User should also themselves focus on leading towards a better security by not sharing their password to any C.S.P officials.

5.3 Unexpected erasure of sensitive information:

The data from the cloud might get unexpectedly erased because of the various security issues or data breaches. The biggest substantial issue which occurs during the usability of the cloud system's is that the hackers hack the system, might it be from SQL injection, might it be from Password Hacking, might it be from cyber activism. If a CSP doesn't ensure three key features: Confidentiality, integrity and availability of data. No matter would it be, if the data from the cloud gets hacked. It will be the biggest and the most dangerous issue ever that sensitive data of an organization or any individual gets hacked. This occurs in the cloud system every now and then and an unexpected erasure of the sensitive data of any professional could

be as much devastating as we cannot consider. It might be open, private or hybrid cloud. No matter what it is, if the digital asset gets erased from the cloud? It is and can tend to be the biggest loss for any professional that information stored in high security remote cloud could be a digital asset of an organization. In order to overlook this as a whole, the main issue that occurs is actually the erasure of data from the cloud system. No matter how huge or impulsive the security could be, if it gets hacked it not only hinders the viability of a C.S.P but also the integrity of the digital asset of a professional who has stored his data inside the cloud systems

5.4 Loss of confidentiality of Data:

As the biggest risk for any individual or any organization is the loss to digital assets of an organization. The sensitive information or digital asset of any professional is harmed as the data get erased from the cloud. The loss of Privacy or confidentiality of the data the biggest loss as the data gets into confrontation of cyber terrorists via the cloud. The major sensitive information would get leaked in the market to the competent of any professional. All the data stored in the cloud would be at stake, as it is the major thing to be provided cyber security to the data of all professionals. Though, as the cloud gets hindered so that would be an ample reason behind the loss of privacy of data

5.5 Loss of Integrity of Data:

As the sensitive data would get leaked in the market of competition. The accuracy and consistency and the factualness of the data would get hindered as the data got hacked from the cloud. That is also a major reason as the sensitive information would get tampered. So, one of

the security issues of cloud is also the loss of integrity of data as the erasure of data occurs in the cloud.

5.6 Loss of Availability of Data:

Consequently, as the data gets erased from the system. It would lead to removing the data from a professional's sight, no matter what any professional would try to recover his/her digital asset from the filth of hackers. So, obviously the access to data that is hacked in the cloud cannot be accessed by the user.

5.7 Social Engineering Attacks would also occur to phish the data from Cloud:

In order to sum up, what is actually social engineering? I would first define it before giving the actual manifestation of how it is done and what types of attack would it include while taking out the digital asset stored in the Cloud. Social Engineering is a mental assault against an organization or an individual that intends to misuse individuals' common inclination from CLOUD to confide in others. To put it plainly, the assailant accepts an adjusted sense of self that objectives are required to trust naturally and PHISH the data in all possible ways they can from CLOUD. Social Engineering can occur in numerous ways and can hinder any professional in the maximum possible ways to take out sensitive information from Cloud. It is hard to know that how many ways there are in which cyber mafia scam the firm or an individual from cloud, Cyber Security don't even themselves have the in-depth know-how about the prevailing issues of Social Engineering could occur while using the cloud, though it is underrated but the effects

caused by the Social Engineering from using the cloud and its results are dire. Though, we cannot sum up the ways in which Social Engineering could be done from the cloud. Crooks will frequently take many months becoming acquainted with a spot before coming in the entryway or making a call as they want to hack the data from the cloud. Their planning may incorporate finding an organization telephone list or organization graph and investigating workers on informal communication locales.

5.8 Authorization and Authentication Concerns:

The biggest authorization and authentication issue are also known as the dire security problem while using the cloud. If somehow, any hacker accesses the sensitive data of an organization. It could cause a bigger problem. Security issues on accessing the digital asset of a personnel from a hacker or a cybercriminal could also be a devastating issue for any professional in maximum possible ways, the data could be secured in such a way that no personnel or a hacker could access it without giving the proper authentication and authorization to enter the cloud.

5.9 Unintentional sharing or mistaken sharing of data:

The communitarian highlights of distributed computing mean it is essential to have the option to impart records to various degrees of access; you may need a provider to have the option to see (yet not alter) an agreement, however, empower a contractual worker to make changes to a period logging document. Most distributed (cloud) computing administrations give an assortment of client jobs that you can allot when sharing a record.

5.10 Client Information loss and financial data issues:

One more problem could also be that, any competent of a professional might hack the sensitive information that could might include client information as it is most secretive and the competent of any professional would try their ample best to get that data in any-way so one more security issue is also the hacking of sensitive information of a professional from the cloud system. It could emerge as a biggest danger for any professional or an individual

6. **Figure showing Security issues of Cloud Computing**

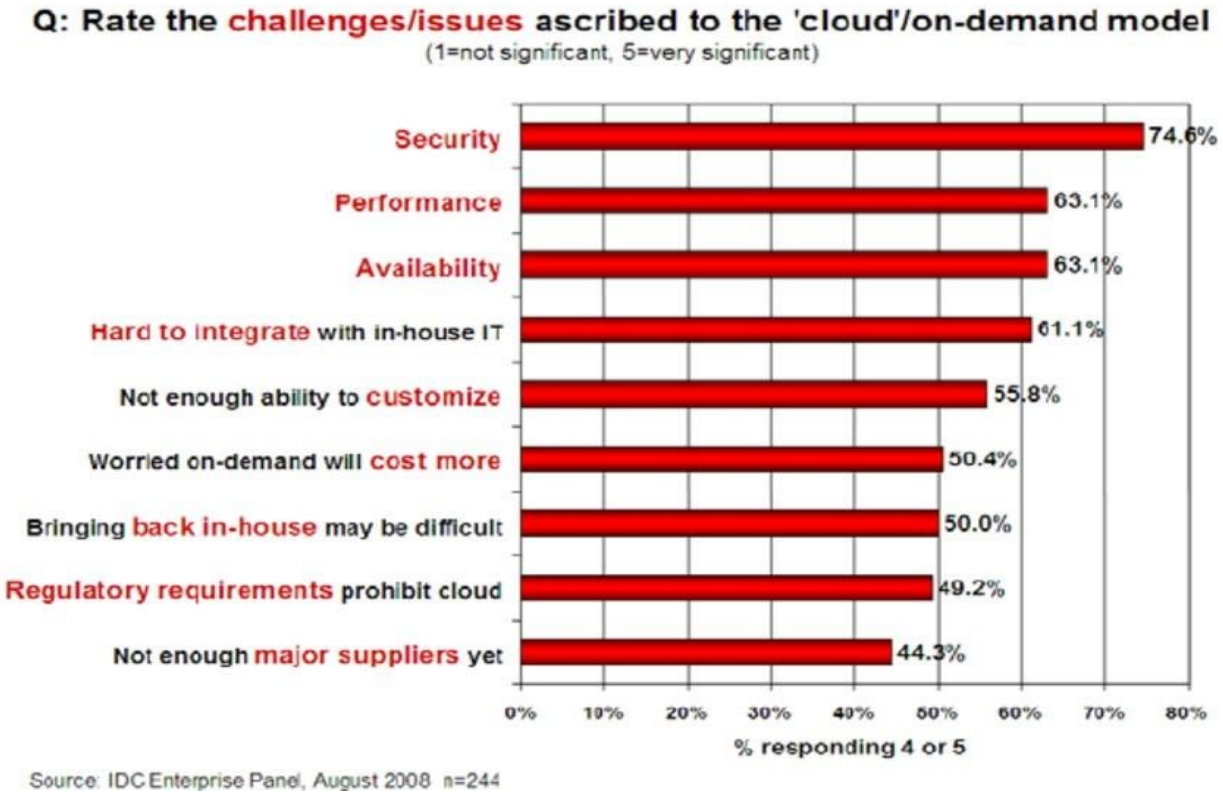

figure 2 (INFO, IDC; 2008)

7. **Conclusion:**

Therefore, we have defined almost 10 security issues and 10 security advantages of Cloud Computing as a whole. All the possible aspects are made sure to be concluded. Cloud Computing is a technology and every technology does have a vulnerability or security issues. To conclude it, the mandate of assuring, of all possible aspects are made sure when it comes to the actual main idea of the report, it is centralized across the manifestation of both positive and negative impacts of Cloud Remote Security issues and advantages. It leads to System Powerlessness (Vulnerabilities), erasure of sensitive information, issue of privacy, integrity, availability, authentication, authorization, social engineering and loss of client data and information are highlighted as major issues of cloud computing

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 var authorBlock = document.getElementsByClassName('main-article-author v2')[0]; var innerHtml = 'Published: 07 June 2010 0:00'; var authorDateDiv = document.createElement('div'); authorDateDiv.className = 'main-article-aut. (n.d.). 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)