RESEARCH ARTICLE

NORTH AMERICAN ACADEMIC RESEARCH (NAAR) JOURNAL
2021 AUGUST, VOLUME 4, ISSUE 8, PAGES 50-58
https://doi.org/10.5281/zenodo.5218565

Research on Security and Vulnerabilities in Cloud Computing

Ahsanul Haque[1]

[1]School of Mathematics and Computer Science , Guangxi Science and Technology Normal University, 966 Tiebei Avenue, Laibin, 546199 Guangxi,China,

OPEN ACCESS

Accepted August 13,2021
Published August 19,2021

***Corresponding Author:**
Ahsanul Haque
ahsanulhaque1998@outlook,com

DOIhttps://doi.org/10.5281/zenodo.5218565

Pages: 50-58

Funding: Self

How to cite this article (APA):
Ahsanul Haque(2021). Research on security and vulnerabilities in cloud computing.*North American Academic Research, 4(8)*, 50-58.doi:**https://doi.org/10.5281/zenodo.5218565**

Conflicts of Interest
There are no conflicts to declare.

ABSTRACT

Cloud computing is a ground place for big enterprise companies that brings together companies' assets on a versatile stage to give customers the ability to store as much data as possible in cloud storage without any hassle, but apart from the positive sides. There have been a lot of data breaches & it’s still happening. This paper outlines what cloud computing is, the different cloud deployment models & the main security risks and issues currently present within the cloud computing industry.

Cloud computing became such an important part of the technology industry that nowadays most companies are moving on to cloud platforms. Big companies have such good cloud storage and rates for other small companies for which a lot of small companies are moving to the cloud and not only because of the low rate but also the fact that they don't have to do anything for physical storage. Since everything from user data to local database is managed by the cloud companies, it saves a lot of money and space for smaller companies to move on to the cloud. But is the cloud safe as the big corporation suggests? According to my research, some matters are making the cloud vulnerable in terms of security for the users data and other personal information that might get into the hands of a hacker easily.

Keywords: CLOUD COMPUTING. NETWORK SECURITY, CLOUD VULNERABILITIES.

Introduction

Cloud service suppliers give opportunities for organizations to make their resources available online for the organization's customers. Cloud computing allows companies/organizations to benefit from porting their current/existing systems to an online cloud-based environment. Where they can be accessed by anyone with the required privileges. The most appealing benefit and advantage of cloud service are that cloud service providers take care of the hardware, software & networking, including the associated cost. The service providers then 'rent out' what the organization requires. This means that the company will only ever use the resources necessary. Service providers will have the hardware & software setup to enable them to scale far and beyond what companies/organizations will require, because of this, the providers will be able to offer similar resources to multiple companies which they offer at a reduced price. Cloud computing is rather a technology that has been out for quite a while now, but rather a new delivery model for information and services using existing technologies. Which uses the Internet infrastructure to allow communications between client and server-side services/applications. Service providers offer cloud platforms for their customers to use and create web services. It is somehow like an internet service provider (ISP) business model that offers customers high-speed broadband to access the internet. Cloud service providers (CSP) and Internet service providers (ISP) both offer services. The CSPs provide a layer of abstractions between the computing resources and the low-level architecture involved. Customers do not own any physical infrastructure but merely pay a subscription fee either monthly or annually depending on the CSP's payment packages for which the CSP grants them access to their infrastructure and cloud resources. The key concept is that customers can reduce expenditure on resources like software licenses, hardware, and other services (e.g. email) as they will obtain these things from one source. Cloud Service Providers. Recent studies have found that disciplined companies achieved on average an 18% reduction in their IT budget from cloud computing and a 16% reduction in data center power costs (McFredie,2008). There are two initial types of cloud computing, Public Cloud and Private Cloud. Within Public Cloud, computing companies pay a yearly subscription to an external company such as Microsoft's Azure cloud database and Amazon's Web Services (AWS) towards storing data and facilitating the running of application programs. Many companies share an equivalent infrastructure within the general public Cloud, and therefore the term given to the present is Multi-Tenant Architectures. This term is significant because a server is up into virtual servers which are software-controlled slices allocated to customers. In the extract, one server will turn into many servers for many customers. The Private Cloud would be the next progression for many companies as the Private Cloud is in-part managed in-house and is considered a Hosted or Corporate cloud. The cloud is always managed within the company's domain and data storage which is centralized while replacing the company's previous infrastructure as the network becomes virtualized. Most data storage is handled in-house because of its sensitivity which must be protected at all times. This is the most secured option and the most expensive but still cost-effective compared to their older structures in which the companies maintain themselves. As Public Cloud is taken into account a multitenant architecture the Private Cloud is taken into account a Proprietary Architecture which provides hosted services to a limited number of individuals behind a firewall. This firewall is found at the network gateway server. Physical hardware resources like Servers are only allocated to one customer. the hearth wall allows public internet access also accommodating VPN Virtual Private Networks allowing company employees to attach to the corporate intranet safely and securely from their homes. The added feature of a VPN is the ability to use public networks a touch just like the web and believe private leased lines. These restricted access networks utilize the same cabling and routers as a public network are categorized within an honest area network. Virtualization to this extent could even be a relatively new concept within the IT industry, which has taken off since the end of 2005, the three main areas where virtualization is showing the simplest significance is within Virtual Networks, Storage Virtualization, and Server Virtualization. The combination of those three important elements provides autonomic computing within the IT environment and is practically self-managing saving cost an incentive. A methodology within network virtualization is employed to mix the supply of resources into a network by ending the available bandwidth and, into channels. Each channel is independent of one another. The breaking up of channels helps towards performance as each one can be assigned and reassigned to a different device or server in real-time. Virtualization disguises the true complexity of a network because it breaks up into manageable parts. The pooling of physical storage is storage virtualization from multiple network storage devices into what could be considered as one singular storage device. This pooling memory device is managed by a central console. The making of server resources including the quantity and identity of individual physical servers, processors, and operating systems from server users is server virtualization. It is designed and implemented in a way that the user does not have to manage the complexity of server settings while increasing resources by sharing and maintaining the capacity to expand. Combinations of those three important elements provide autonomic computing during which the IT environment would manage itself. While within the private cloud there would be an administrator who oversees the running of the virtual network.

A summary of the key aspects of cloud computing

The cloud : There are five key attributes for Cloud Computing that grants some advantages over technologies alike and these attributes are :

Shared resources (Multi Tenancy) : Although previous computing models took up dedicated resources that were dedicated to a single user or owner. Cloud computing is based on a business model in which resources are shared in the network,host and application level.

Immense scalability: Cloud computing provides the power to scale to tens of thousands of systems, also because of the ability to massively scale bandwidth and space for storing.

Flexibility: Users can rapidly increase and reduce their computing resources as required, also release resources for other uses once they are not any longer required.

Easy subscription model: The subscription and payment depend on the users as they can rapidly increase and decrease their computing resources as needed while releasing new resources for other uses when they are no longer required. Users can end/stop their subscription at any time.

Self-supply of resources: Users can supply themselves with resources, such as additional systems (processing capacity, software & storage) and network resources. There is a call around cloud computing, as users of cloud services have to pay for what they use & the resources they need to cope with demanding situations can be adjusted, which depends on the demand. It is recognized as the Cloud Delivery Model (SPI - see figure 1). The cloud delivery model consists of three services, which are known as Software-as-a-service (Saas), Platform-as-a-service (Paas), and Infrastructure-as-a-service (Iaas)

Software-as-a-service (Saas) provides users to make use of various applications from the cloud rather than using applications on their computer. The cloud service providers (CSP) usually provide some software development environment for applications for development for use within the cloud. The application programming interface (API) which the users use to access and interact with the software allows the user to use the software without having to stress about how or where the info is being stored or what proportion of disc space is out there because the cloud service provider will manage it for them.

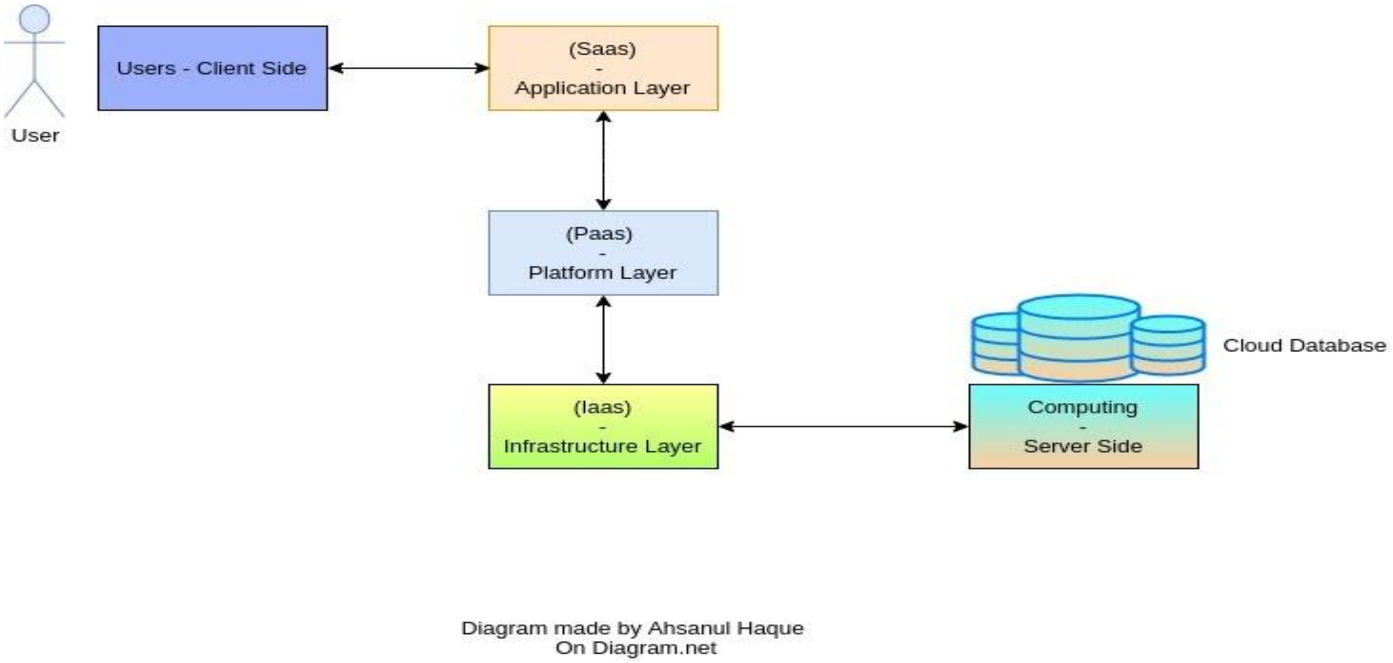

Figure 1: Presenting layers of cloud delivery model

platform-as-a-service (Paas) functions at a smaller level than software-as-a-service (Saas). It is in control of managing the storage, measuring bandwidth, and computing resources that are accessible for the applications. It regains the resources needed to run the software and dynamically scales up these resources when more is needed. Platform-as-a-service (Paas) holds a key attribute of the cloud as the self-provisioning of resources. Infrastructure-as-a-service (Iaas) dynamically measures bandwidth and server resources for the cloud. This service allows the cloud to operate during high traffic/demanding situations as resources are dynamically increased as they are required. The pay-as-you-go system plays a massive role in this service as the user is charged for how much bandwidth or server resources are needed.

There are three main sorts of cloud deployment models. public, private and hybrid clouds.

Public clouds - The most common type of cloud. This is where numerous customers can access cloud services/web applications and services over the internet. Each customer has their resources which are dynamically provisioned by a third party seller. The third-party seller hosts the cloud for numerous customers from numerous data centers, controls all the security, and provides the hardware and infrastructure for the cloud to operate. The customer has no control or insight into how the cloud is managed or what infrastructure is out there.

Private clouds - Imply the approach of cloud computing on a private network. They give users the benefits of cloud computing without some issues that are on public clouds. Private cloud enables the users of complete authority over how data is being maintained and the security measures that are in place. This as a matter of fact leads to users having more confidence and control, but there is a major issue with this deployment model, that is the users have huge expenses as they have to pay for the infrastructure to run the cloud and also manages the cloud themselves.

Hybrid clouds - Blending both private & public cloud services (See figure 2) while in the same network. It gives the users (Organizations) the benefit from both deployment models. Example, an organization can hold sensitive information on their private cloud and use the public cloud for handling huge traffic in demanding situations.

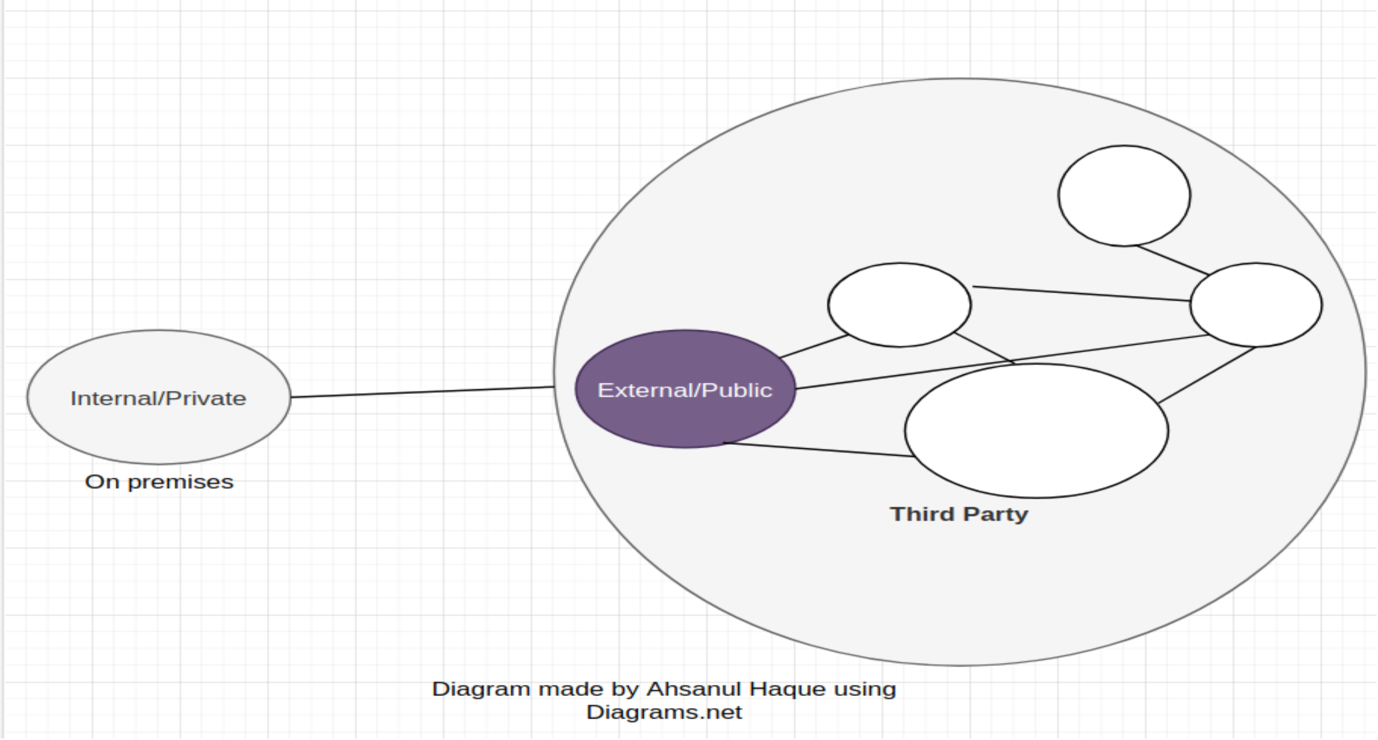

Figure 2 : Showing Hybrid Cloud Deployment Model Security in the Cloud

One of the chances that people detect the cloud is the cloud service providers (CSP)'s might not be able to manage with the large scale of or the infrastructure will not be able to scale properly with large amounts of usage (Ohlman et al., 2009). Privacy is important for organizations and their users especially when an individual's personal information or sensitive information is being stored but it isn't completely understood whether the cloud computing infrastructure will be able to support the storing of sensitive information without making organizations liable for breaking privacy regulations. Many believe that cloud authorization systems are not robust enough with as little as a password and username to gain access to the system, In many private clouds, usernames can be very similar, degrading the authorization measures further. If there was private/sensitive information being stored on a private cloud then there is a high chance that someone could view the information easier than many might believe. The customer is advised to only give their data or use the cloud provider's system if they trust them.

As companies move onto Cloud Computing with the incentive of low cost by the aggregation of servers and data into a centralized location which can translate to severity toward aggregation of risk. There have been significant incidents of successful disruption on Cloud Networks due to hackers. Google was the target of attacks aimed at stealing intellectual property and identifying that human-rights activists were targeted seeking reforms in China. The incident prompted the Internet search giant to re-evaluate whether it will continue doing business in the country (MarketWatch, 2010). Google's Infrastructure is mainly in the Cloud and companies with high profiles become bigger targets. The resources such companies have toward security investment are considerable and Google supplies software security also more so to business. Attacks to data have not just been on Google but companies from a wide range of businesses–including the Internet, finance, technology, media, and chemical sectors–have been similarly targeted (Everiss, 2010).

Cloud service providers believe encryption is the key and can help with a lot of the security issues but what comes along with the benefits of encryption are the pitfalls as encryption can be processor intensive. Encrypting is not always full proof for protecting data, there can be times when little glitches occur and the data cannot be decrypted leaving the data corrupt and unusable for customers and the cloud service provider. The clouds resources can also be abused as cloud providers reassign IP addresses when a customer no longer needs the IP address. Once an IP address is no longer needed by one customer after a period of time it then becomes available for another customer to use. Cloud providers save money and do not need as many IP addresses by reusing them, so it is in the cloud provider's interest to reuse them. Too many of these idle/used IP addresses can leave the cloud provider open to abuse of its resources. There is a period between an IP address being changed in DNS and the DNS caches holding the IP address getting cleared. If these old/used IP addresses are being held in the cache then they can be accessed which would grant a user access to the resources that are available at the IP address. Also another customer of the same cloud provider could potentially gain access to another customer's resources by navigating through the cloud provider's networks, if no/little security measures are put in place. Data and information is like a currency for cyber terrorists/crooks and clouds can hold enormous amounts of data so clouds are becoming an a attractive target for these crooks which is why cloud security must be top notch and should not be overlooked (Wayner, 2008).

Cloud API's and software-as-a-service are still evolving which means updates can be frequent but some clouds do not inform their customers that these changes have been made. Making changes to the API means changing the cloud configuration which affects all instances within the cloud (see figure 3). The changes could affect the security of the system as one change could fix one bug but create another. The customers of the cloud provider should enquire if any updates are made and should ask about what security implementations have been put into place to secure their data and what exactly has changed with the system. Some ways to verify if the company is right for your information is to ask if there is a third party auditing their cloud or do they have any security certificates.

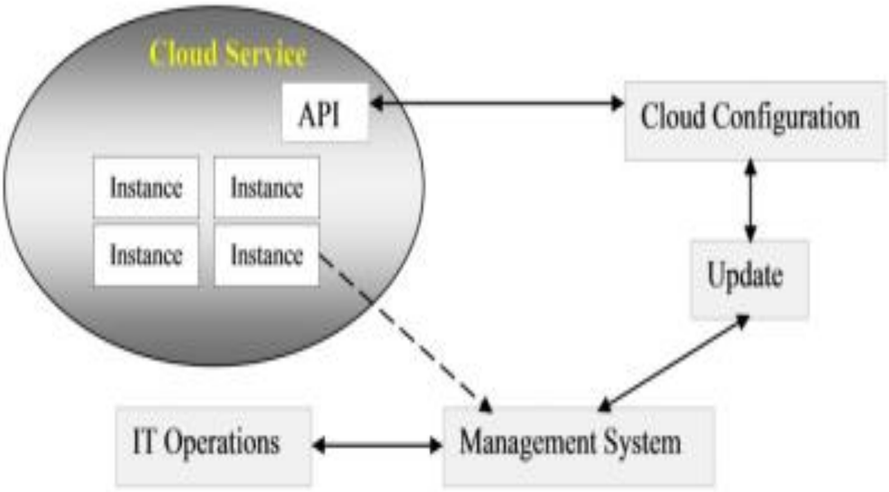

Figure 3: Showing relationships of the cloud API and other key cloud components

If a cyber criminal hacks into the cloud provider and data which belongs to the customer has been copied off the server then the customer may not know. The cloud provider will have access to the server logs and the customer will not. Multiple customers may be sharing the resources of the same servers and one customer could be using multiple hosts potentially every day. This would make tracking of the unauthorized access of the data to be nearly impossible for the cloud service provider as the data can been very widely spread throughout the cloud providers networks. Unless the cloud provider has developed some sort of monitoring software which can group/sort processes which have occurred for each user then this could be a large security risk and make attacking clouds even more attractive for cyber criminals. Most customers will not know where their data is being stored by the cloud provider. This poses a number of issues especially if the information is important or valuable. Customers who are worried about security should ask their cloud provider where the physical servers are held, how often are they maintained and what sort of physical security measures have been taken (e.g. biometrics or PIN access) to restrict access to the server resources. There is a chance that the data will be held in another country which means the local law and jurisdiction would be different and could create a different security risk, as data that might be secure in one country may not be secure in another (Staten, 2009). By looking at the different views on data privacy between the US and the EU, this security risk becomes more evident as the US has a very open view on the privacy of data. The US Patriot Act grants government and other agencies with virtually limitless powers to access information including that belonging to companies whereas in the EU this type of data would be much more secure, so local laws and jurisdiction can have a large affect the security and privacy of data within a cloud (Mikkilineni and Sarathy, 2009).

Conclusion

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their existing customers on the level of security that they provide on their cloud. The cloud service providers need to educate potential customers about the cloud deployment models such as public, private and hybrids along with the pros and cons of each. They need to show their customers that they are providing appropriate security measures that will protect their customer's data and build up confidence for their service. One way they can achieve this is through the use of third party auditors. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. Plugging in existing security technology will not work because this new delivery model introduces new changes to the way in which we access and use computer resources. We must remember that when a corporation loses sensitive data, it is quite often an inside job therefore organizations must consider carefully who they are handing their sensitive data. In the standard model of data remaining in-house, they can monitor closely the use of data and irregularities within staff. They can also set and unset the credentials required to access this data, enabling them to remain in control. However, in the cloud, they must place a lot of trust in the service provider, in their abilities to employ reliable members of staff and only offer the required security privileges to those who it deems necessary .A degree of trust will always remain, however there are external security standards (ISO27001), and if a cloud service provider conforms to this standard, they will be able to be audited to ensure the compliance. This will give considering companies an added boost of trust as they can ask to view any previous audits.

Acknowledgments

The author would like to acknowledge and thank his supervisor Assoc. Prof Ms Pan Changchun from

Computer Science Department of Guangxi Science and Technology Normal University, Laibin, China for rigorously overseeing the paper.

References

1. "What is Cloud Computing - Amazon AWS." https://aws.amazon.com/what-is-cloud-computing/.
2. "What is Cloud Security? Understand The 6 Pillars | Check ...." https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/.
3. "What is different about cloud security? - Red Hat." https://www.redhat.com/en/topics/security/cloud-security.
4. "What is Cloud Security? How to Secure the Cloud | McAfee." https://www.mcafee.com/enterprise/en-us/security-awareness/cloud.html.
5. "What are data centers? How they work and how they are ...., https://www.networkworld.com/article/3599213/what-are-data-centers-how-they-work-and-how-they-are-changing-in-size-and-scope.html.
6. "Cyber Crime — FBI." https://www.fbi.gov/investigate/cyber.
7. "How hackers breach unlocked cloud server databases - The ...." https://www.washingtonpost.com/technology/2020/03/02/cloud-hack-problems/.
8. "Types of Cloud Computing | Ethical Hacking - GreyCampus." https://www.greycampus.com/opencampus/ethical-hacking/types-of-cloud-computing.
9. "Hacking and Securing Cloud Infrastructure - NotSoSecure." https://notsosecure.com/hacking-training/cloud-hacking/.
10. "What is cloud computing? Everything you need to know about ...." https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/.