Review on Cloud Computing Security Challenges

Evans Osei-Opoku, MSc
Rym Regaieg, PhD
Mohamed Koubaa, PhD
National Engineering School of Tunis (ENIT),
University of Tunis El Manar, Tunisia

Doi:10.19044/esj.2020.v16n12p63 URL:http://dx.doi.org/10.19044/esj.2020.v16n12p63

Abstract

In this paper, security issues associated with cloud computing are reviewed. Additionally, the types of cloud and service models have also been pointed out. Cloud computing has ruled the data innovation industry as of late. Giant data centers that provide cloud services are been set up due to the global approval of cloud and virtualization innovations. Cloud computing is characterized as a web-based software service since Information Technology (IT) resources like network, server, storage, and so on are based on the Web. Along these lines, cloud computing services can be utilized at any place and whenever on the Personal Computer (PC) or smart mobile phones. In light of the on-demand, adaptable and versatile administration it can give, a considerable measure of companies that beforehand deployed locally has moved their organizations to the cloud. Although cloud computing brings a whole lot of advantages, many security challenges have been brought up to both cloud providers and clients.

Keywords: Cloud Computing, Cloud Security, Data Centre, Computing Services, Privacy, Integrity

Introduction

Cloud computing is the latest trending in the IT industry that transfers computing and data from portable and standalone PCs to huge data centers (Dikaiakos et al., 2009). Given the cloud computing model compared to the former model of computing, cloud computing has several potential benefits. For instance, an organization's cloud data can be increased or decreased based on the demand at hand. Cloud users are provided with computing resources on a pay-as-use basis. Also, storage and retrieval of data can be performed at all times from any location. As cloud computing has the capacity to satisfy any

IT industry resources, many businesses have moved their establishment by adopting cloud services.

Although cloud computing has several advantages, the privacy and safety protections associated with these services are currently the main obstacle to convincing cloud computing services (Sharda, 2013). The main security problem for cloud services is that the data holder may not have the means to control where the information is physically located. Currently, data is important and has uncountable values, keeping such information in an open cloud creates uncertainties about the privacy, availability, and exploitation of data.

The remainder of the paper is organized as follows. In section II, the types and service models of cloud computing are discussed. Section III highlights some of the prominent security concerns in the cloud domain. We conclude in section IV with future works.

Cloud Computing

What is Cloud Computing?

The generally accepted definition of Cloud Computing comes from the National Institute of Standards and Technology (NIST) (Mell et al., 2011) which states "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". In short, it means that end-users are to utilize parts of bulk resources and that these resources can be acquired quickly and easily. Cloud computing is a standout among the most well-known topics and quickly developing an approach in the field of data innovation.

Classification of Cloud Computing

Cloud users are able to utilize the services offered by cloud providers via the internet. An important aspect to consider with the cloud is the proprietorship and utilization of the cloud infrastructure. Cloud infrastructures can be deployed with different methods. Figure 1.0 shows the types of cloud deployments.

- Private cloud: Cloud frameworks owned and regulated by a solitary organization, used in a private network and not accessible for open/public use.
- Public cloud: High-performance and vast infrastructures operated by external companies that provide IT services to numerous customers utilizing the Internet.
- Community cloud: Shared cloud frameworks for particular groups formed by multiple users.

- Hybrid cloud: A hybrid cloud is a blend of both a private and public cloud. Some parts of the service keep running on the organization's private cloud, and the other parts are outsourced to an external public cloud.

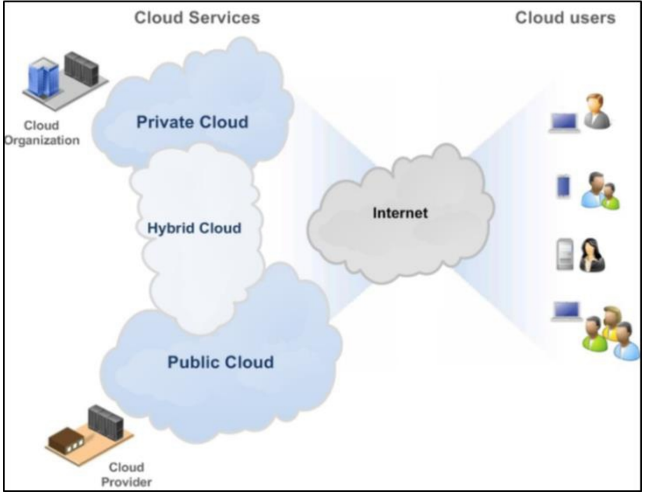

Figure 1.0. Cloud Computing Deployment (Beloglazov et al., 2012)

Classification of Cloud Service Model

Cloud Service Models can be arranged into three sorts:

- Infrastructure as a Service (IaaS) which is likely the most predominant cloud service model. In the case of IaaS, the service provider offers virtualized hardware to users. The virtualized hardware may include a virtual machine (VM), storage space, virtual network. IaaS service providers maintain massive physical re-sources across the world. These physical resources are virtualized by splitting individual resources into several virtualized, isolated resources. This approach maximizes the utilization of individual resources and offers flexibility. Famous IaaS service provider includes Amazon Web Service (2019), Google Cloud (2019) and Windows Azure (2019).
- Platform as a Service (PaaS) provides a software environment in addition to the underlying software. For example, deploying a website requires developers to buy and install hardware, operating systems, development environments, databases, web servers, then develop the website and deploy it. After deploying it, developers need to maintain and monitor it. It is also common to develop an analysis system to display statistics of the website. PaaS service providers simplify this process by offering a configured environment so developers only need to log in and start programming the website which is their core work. This model is a good choice for individual developer and small enterprise which does not have a big IT team.
- Software as a Service (SaaS) is a software model where service providers host applications and make them available to cloud users over the internet. This software does not refer to traditional software needed to be installed

locally. It usually refers to a centrally hosted software and the user accesses it via a thin client or a web browser. IaaS and PaaS services basically serve developers and IT teams but SaaS usually serves personal users and enterprise customers. Typical SaaS service provides include Google Docs (2019) which provides document editing service, Dropbox (2019) which provides file storage service and Netflix (2019) which provides video streaming service.

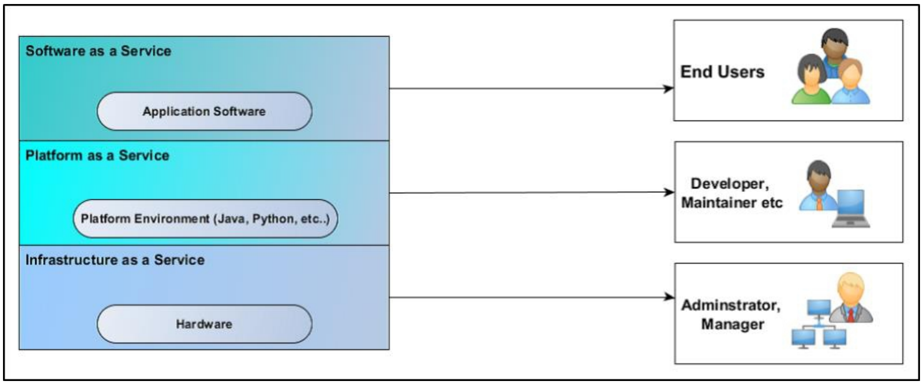

Figure 2.0. Cloud Service Models (Osei-Opoku, 2018)

Cloud Computing Security Challenges

Security is always a major issue as the absence of it has a significant negative impact on ethical, personal and financial harm. Because cloud service providers host data centers in geographically distributed locations, several security issues are raised as cloud users have no idea as to where their sensitive data are stored. In Gartner's survey (Brodkin et al., 2008), more than 72% of the Chief Technical Officers thought it was primarily due to problems with information security and privacy that, cloud services were not used. It is a tough task to persuade especially small businesses of security concerns; as they are not willing to move their infrastructure back into the cloud. The main reason why cloud computing does not develop is mostly that, the companies handle this issue with care and are not prepared to move to cloud storage. For cloud security and privacy to be enforced, both cloud service providers and cloud users must be mindful of the term and conditions associated with cloud data sharing and its services.

At this juncture, some of the security issues associated with cloud computing are as follow:

- Data integrity: Integrity can be referred to as information accessed or changed by unauthorized users. Several institutions share the application or platform on a multi-tenancy basis, making it possible for the users to share information with any other unauthorized user in the cloud, hence resulting in a failure in integrity. For cloud services like SaaS, PaaS, data plays a key role in their provisions. Thus, data integrity is a rudimentary task (Baker et al., 2011).

- Data Privacy: The privacy of data is vital in the cloud computing domain. For many organizations, storing valuable information on their site is more convenient than the cloud. As cloud users have no knowledge as to how their information is stored, data transferred, cloud operations, and the likes, a number of concerns are raised. Whether or how data is shared with third parties, creation and deletion of files, location of information, information backup and who can access the information, to mention a few, are some of the many questions cloud users inquire about.
- Data Breaches: The cloud environment is accessed by multiple users and organizations from anywhere as their data is kept in one location. Sensitive data of the users can be exposed if there is any occurrence of break or cloud problem. Customers using different applications on the virtual machines could share the same database because of its multi-tenancy, and any compromising incident that occurs will affect other users sharing the exact same database (Hubbard et al., 2010). According to the 2011 Data Breach Investigations Report by Kumar and Arri (2013), 50% of hacking and 49% of malware were identified to be the common causes of da-ta breaches.
- Malicious Insiders: Malicious insiders are authorized staff, who are assigned to administer and maintain the cloud by cloud service providers. Such clients often steal or manipulate sensitive data from cloud organizations, and send this sensitive information to file-sharing organizations. These insiders can be paid for this unethical work. Sometimes service providers are not able to take action against these staff.
- Data Location: For Storage as a Service model, the location of the information is very important. Some cloud users are reluctant to store their sensitive data in the cloud as the location of their data is unknown. This is one of the common concerns encountered by most organizations, thus, leading to security issues, legal issues, and regulatory compliance requirements. This has become one of the prominent challenges as a result of untrusted cloud service providers.
- Resource Sharing: One of the indispensable features of cloud computing is resource sharing. According to Wueest, Barcena and O’Brien (2015), 75% of security issues happen as a result of resource sharing. In the case where a malicious VM is found in the cloud, it can cause resource starvation to the anticipated VM. Therefore, the problems associated with resource sharing need to be addressed.
- Data Storage: Cloud computing offers high data mobility. And due to that, most cloud users have no idea of the location of their information. Cloud computing is not just a database third-party, therefore traditional database security solutions cannot be implemented directly. Furthermore, it is difficult to follow a cryptographic approach as it will mean cloud users lose their control of cloud data (Wang et al., 2010). The proper data storage check in the

cloud must, therefore, be performed without explicit knowledge of cloud data. Finally, cloud computing is done in a cooperated, simultaneous and collaborative data center. Hence, to achieve a secured cloud data storage, distributed protocols must be incorporated.

Conclusion

We looked at the security challenges in cloud computing in this paper. Cloud computing is a global innovation that offers easy access across web services to high-performance computing tools and processing infrastructure. Cloud computing provides governments, companies, private and individual users the opportunity for flexibility, cost savings, and improved performance. This paper addresses the important safety issues and obstacles that cloud computing is currently facing. In the future, Cloud computing will lead the way in supporting a stable, digital and cost-effective IT solution. Hence, we look at proposing new models or algorithms that will help make cloud services safe to use.

References:

1. Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud computing: Distributed internet computing for IT and scientific research. IEEE Internet computing, 13(5), 10-13.
2. Rahul, S. Sharda,"Cloud Computing: Advantages and Security Challenges". International Journal of Information and Computation Technology", ISSN, 0974-2239.
3. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
4. Beloglazov, A., Abawajy, J., & Rajkumar Buyya, R. (2012). Energy-Aware Resource Allocation Heuristics for Efficient Management of Data Centers for Cloud Computing. Future Generation Computer Systems, 28(5):755-768
5. Amazon Webs Service https://aws.amazon.com/about-aws/
6. Google Cloud Platform (2019) https://cloud.google.com/
7. Microsoft Azure (2019) https://products.ofice.come/en-us/word/
8. Google Docs (2019) https://google.com/doc/about
9. Dropbox (2019) https://dropbox.com/about/
10. Netflix (2019) https://media.netflix.com/en/about-neflix/
11. Osei-Opoku, E. (2018). An Accurate Power Consumption Model for Cloud Computing Data Centres (Unpublished master's thesis). National Engineering School of Tunis (ENIT), University of Tunis El Manar, Tunis, Tunisia
12. Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. Infoworld, 2008, 1-3.

13. Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., ... & Tippett, P. (2011). 2011 data breach investigations report. Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf, 1-72.
14. Hubbard, D., & Sutton, M. (2010). Top threats to cloud computing v1. 0. Cloud Security Alliance, 1-14.
15. Kumar, P., & Arri, H. S. (2013). Data location in cloud computing. International Journal for Science and Emerging Technologies with Latest Trends, 5(1), 24-27.
16. Wueest, C., Barcena, M. B., & O'Brien, L. (2015). Mistakes in the IaaS cloud could put your data at risk. Symantec.
17. Wang, C., Wang, Q., Ren, K., & Lou, W. (2010, March). Privacy-preserving public auditing for data storage security in cloud computing. In 2010 proceedings ieee infocom (pp. 1-9). IEEE.