Timothy Kang
Due Date: 4/25/18
ITMO 441-02
Illinois Institute of Technology

Cloud Computing and Security

Whether one is working for a business or doing a simple homework assignment for school, one might have heard of the term "the cloud." To many, the cloud and the Internet have been used interchangeably, and many make use of numerous cloud services provided by well-established companies such as Google and Amazon. However, a majority of people do not know exactly what the cloud is and how it is being managed by something known as cloud computing. In addition, the security issues that plague cloud computing are unknown to the average person. These concerns should be addressed and understood by both the customers and the cloud providers. Before delving into cloud security, it is necessary to fully understand cloud computing.

What exactly is cloud computing? "It is a macrostructure distributed computing instance with minimal effort and cost in highly available and dynamically scalable computing resources" (Sinanc & Sagiroglu, 2013). Simply put, this service allows one to make use of virtualized resources over the Internet and only pay based on usage without the need to buy your very own server and software. Despite this being a relatively new and upcoming technology, the idea of the cloud originated from the 1990's when providers utilized Virtual Private Network services for data communications and the term "telecom cloud" was coined (Boampong & Wahseh, 2012). This would be the beginning which would one day lead to popular cloud computing services such as Amazon-EC2 and Google Docs.

While knowing the history and definition of cloud computing is nice, it is of vital importance to understand the cloud computing model, the actors, and the many characteristics it

has since there are security issues that stem from this. There are three actors that make up the cloud computing model: the cloud provider, service provider, and the customer. The infrastructure that is used by the customer is provided by the cloud provider. This infrastructure serves as a platform for applications and services that are given by the service provider. Lastly, the customer can make use of these applications, services, and infrastructure to do as they please (Sinanc & Sagiroglu, 2013). Clearly, these actors are reliant on each other in the model, and it would be incomplete and not function as intended if any of them were absent. The National Institute of Standards and Technology further broke down the cloud model. According to them, the model consists of "five essential characteristics, three service models, and four deployment models" (Sinanc & Sagiroglu, 2013).

First off, the five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Sinanc & Sagiroglu, 2013). On-demand self-service means that the customer is capable of using the cloud computing services for their own purposes wherever and whenever as long as they have Internet access. Since the Internet can be seen as a ginormous network and the cloud services are available on this network, broad network access is seen as a necessary characteristic. Resource pooling is a characteristic because the service provider allows for multiple resources to be available on the cloud infrastructure. In addition, access to the Internet is not limited to one person at a time. Therefore, rapid elasticity is an essential characteristic so that the service can be scaled based on factors such as number of users and their usage of resources. Lastly, being able to monitor and measure this usage of resources is important for this model to work.

Next comes the three service models with Infrastructure as a Service (IaaS) as the lowest layer, Platform as a Service (PaaS) as the middle layer, and Software as a Service (SaaS) as the

highest layer (Bhadauria, Chaki, Chaki, & Sanyal, 2014). IaaS simply provides the infrastructure and computing resources which "is usually in the method of platform virtualization" (Boampong & Wahseh, 2012). Platform virtualization means that the resources come from managed virtual machines which are scaled based on usage. Some examples of IaaS solutions include Amazon Web Services, Windows Azure, Microsoft System Center, and Citrix CloudPlatform (Sinanc & Sagiroglu, 2013). PaaS serves as a way to control the numerous cloud services that are made available to consumers. In addition, by using this service, customers are able to create applications since it includes a software execution environment (Bhadauria et al., 2014). SaaS is something an everyday person is more accustomed to. Simply put, the consumer is able to use software over the Internet without having to download these applications onto the hard drive; software maintenance is clearly not a problem thanks to this service. A student might be writing their paper on Google Docs or sending an excuse for an absence through Gmail. Both e-mail clients and word processors such as this make use of SaaS. IaaS is considered "the most established cloud service model" since it offers a "wide variety of products and advanced capabilities" such as automated scalability and on-demand provisioning (Vaquero, Rodero-Merino, & Morán, 2011).

There are many cloud computing platforms and systems that all serve different purposes. Google's BigTable "is a distributed and large-scale storage system for managing structured data" (Sinanc & Sagiroglu, 2013). On the other hand, Amazon's EC2 is used for application hosting. Despite these differences, each can be categorized into a deployment method: private cloud, community cloud, public cloud, hybrid cloud, or virtual private cloud. The fifth deployment method which is virtual private cloud is not covered by NIST. Private cloud infrastructure is available for a specific customer or organization. Management of this service is done by a third-

party service provider or the organization can choose to do it themselves (Bhadauria et al., 2014). Public cloud allows for resources to be open to the public, so it can reach many different consumers. Unlike private clouds, public clouds are "generally owned and managed by the service provider" (Boampong & Wahseh, 2012). Just like the name implies, community cloud infrastructure is shared within a community which could consist of multiple organizations with a similar purpose. Hybrid cloud is a combination of two or more deployment methods, but they are naturally linked so that neither side is affected in a negative way when transferring data. Lastly, virtual private clouds are when a "service provider [utilizes] public cloud resources and infrastructure to create a private virtual cloud, usually via VPN connectivity" (Boampong & Wahseh, 2012).

Based on seeing the different models and capabilities of cloud computing, one can see the many perks of using it in any kind of setting. With state of the art techniques such as virtualization, web service, SOA, and application programming interface, the appeal of cloud computing continues to grow in a positive way (Bhadauria et al., 2014). With virtualization, an environment could be created, where hardware and software limitations are not a problem for either everyday users with basic personal computers or corporations that don't wish to spend more than what they need. With web service and Service Oriented Architecture, services could be accessed over the web and organized in such a way that multiple services can be used to perform specific tasks (Bhadauria et al., 2014). Finally, APIs allow cloud services to both deploy and be configured for users. Without a doubt, cloud computing has many pros to its usage; nevertheless, the question that arises is, "from a security viewpoint, what kind of issues could it possibly have?"

Just like with any other emerging technologies, this one has its flaws too. One instance is when hackers got ahold of user account information and files under those accounts from Dropbox which is a "popular cloud storage and synchronization service" (Goldsborough, 2013). This was possible because some people tend to use the same login information for multiple sites which made it possible to get a hold of their Dropbox information when another site with the same information was compromised. Contrastingly, Amazon's video streaming service and even Netflix which are both cloud streaming services along with Gmail which, as stated before, is a cloud email service had a period where service went down which prevented users from watching movies or sending emails (Goldsborough, 2013). These are a few of many more instances where cloud threats have been seen and affected one or more actors of the cloud computing model. This is why it is necessary to see and understand the main security threats along with the conceivable ones that can occur within the cloud.

There are six security requirements to information security (Fernandes, Soares, Gomes, Freire, & Inácio, 2014). Identification and authentication deal with ensuring the identify of the user and making sure that they are the person they claim to be. Authorization determines permissions and what a user can do. Confidentiality makes sure that only those that are authorized have access. Integrity is confirming that no data has been tampered with. Non-repudiation is to guarantee that someone cannot deny what has been said or done. Lastly, availability regarding security deals with making sure that the service is up and running without any downtime. While these requirements do play a role in a more traditional data and communication security setting, it is also very important for cloud computing. In addition to the six, there are other threats and precautions that can be observed.

"The main reasons of risks and challenges for cloud computing are that users delegate

authority cloud providers, and having an environment where resources are shared by multiple customers/users" (IOVAN & IOVAN, 2016). Topics such as multi-tenancy and elasticity should be considered since multiple users have the capability to share common resources and their degree of usages differ from person-to-person. An example of multi-tenancy is a college dorm where everyone is a "tenant" residing in a different room but have access to the same resources such as electricity. The dormers have the ability to decide on how much electricity they wish to use but they may decide that they wish to keep this information confidential from other dormers. Similarly, in a cloud setting, it is important for there to be "isolation among tenant data" so that internal or external attacks can be avoided (Sinanc & Sagiroglu, 2013). After all, this goes back to the previous issue of confidentiality. Furthermore, policies, software security, and physical security also serve as issues for cloud computing.

Policies are required to "protect people and information, and set the rules for expected behavior by users, system administrators, management, and security personnel" (Boampong & Wahseh, 2012). For example, no matter how secure a network is from the outside, it does not mean it is secure from inside threats such as an employee with nefarious intentions and access to sensitive data. Software security is a difficult thing to enforce because of how complex code can get, especially with millions of lines of code. Losing valuable data, experiencing server downtime, or unauthorized access to sensitive data can be detrimental to both the consumer and the provider. Physical security deals with keeping the data centers secure. These data centers are "facilities [that] have an umpteen number of servers that compute and store customer data" (Fernandes, Soares, Gomes, Freire, & Inácio, 2014). Geological, environmental, political, governmental, and energy-saving aspects should all be considered when creating a data center; having a data center in an extremely hot and humid earthquake-prone area with a government

uprising would probably not be a good idea. Furthermore, on-site security along with restricted access to computation servers, storage servers, and network equipment is needed. Network security countermeasures should also be implemented such as firewalls, IPSes, IDSes, and honeypots. Firewalls and IPSes are used for "[preventing] security incidents," IDSes are used for "[alerting] malicious intrusion attempts," and honeypots help to "create distractions for attackers and therein learn their movements" (Fernandes et al., 2014). By having a strong physical foundation, cloud providers can "assure that the cloud uptime is very high, reaching 99.99% and is fully fault-tolerant" (Fernandes et al., 2014).

Clearly, there are many vulnerabilities and factors to take into account. Many surveys have been conducted to see the main security threats of cloud computing. One threat is the possibility of using services for nefarious purposes such as hosting botnets. Insecure interfaces and APIs, malicious insiders, shared technology issues, data loss and leakage, and account or service hijacking are all possible threats within the cloud infrastructure (Vaquero et al., 2011). There are many more general issues that can affect the cloud such as man in the middle attacks, denial of service, and DNS hacking. An example of this is when "Amazon S3 suffered data corruption due to a flaky border gateway router" (Vaquero et al., 2011). Over the Internet, there are many people that look for and exploit vulnerabilities. Whether an issue is cloud-specific or not, it should all be taken into consideration so that relationship between the providers and consumers continues without a problem and the trust between them is unbroken.

There is absolutely no way for a system of any kind to be 100% secure. Whether its by human error or technological flaws, security issues will continue to exist. However, there are schemes that can be deployed so that data security can be ensured to a certain extent. First off, using an encryption scheme will help with preventing any stored data from being compromised

easily (Goldsborough, 2013). Limited access to service providers and stringent access controls will also be beneficial for preventing unwanted eyes from observing sensitive information. Since servers can experience downtime, backups and redundant data storage are always needed and should be kept up to date. No customer wants their data to be lost or out of reach when a server is down, and no provider wants to lose a customer which could lead to a bad reputation and decrease in revenue. Another possible scheme is distributed identity management and user security that is maintained by Lightweight Directory Access Protocol or published APIs (Bhadauria et al., 2014). These methods won't ensure complete data security but can still be advantageous for every actor of the cloud model.

Regardless of what security measures are put into place, it is important to remember the main goals of security of the cloud. It is not just one goal but multiple goals that encompass cloud security. Protecting data from unauthorized access and modification, preventing unauthorized access to resources, ensuring isolation and availability, ensuring network security and confidentiality, and putting in effort to monitor, detect, and act on threats are all main goals of cloud security (IOVAN & IOVAN, 2016). Without a doubt, there is a lot to consider when it comes to cloud computing for both users and providers.

Cloud computing has become an integral part of our lives. Advantages such as "reduced hardware and maintenance cost, accessibility around the globe, flexibility" and the need to not worry about upgrading software make cloud computing very desirable for users ranging from students to huge corporations (Bhadauria et al., 2014). However, it is not safe to say that there are no flaws to this technology, especially when it comes to security. Issues such as data leakage or critical bugs must be ensured to never happen. These issues should not discourage users from ever using cloud services. Instead, careful consideration of the pros and cons should be done to

see if the risks outweigh the advantages. All-in-all, cloud computing is vulnerable to threats of different levels, but by knowing about the possible issues, preparing for it, and actively monitoring and acting upon these threats, it is a technology that will continue to improve and continue to be a stable part of our personal and professional lives.

References

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2014). SECURITY ISSUES IN CLOUD COMPUTING. *Acta Technica Corvininesis - Bulletin Of Engineering*, *7*(4), 159-177.

Boampong, P. Wahseh, L. (2012) Different Facets of Security in the Cloud. *CNS '12 Proceedings of the 15th Communications and Networking Simulation Symposium,* (5).

Fernandes, D., Soares, L., Gomes, J., Freire, M., & Inácio, P. (2014). Security issues in cloud environments: a survey. *International Journal Of Information Security*, *13*(2), 113-170. doi:10.1007/s10207-013-0208-7

Goldsborough, R. (2013). How Sound is the Cloud?. *Teacher Librarian*, *40*(3), 68.

IOVAN, Ş., & IOVAN, A. A. (2016). CLOUD COMPUTING SECURITY. *Fiability & Durability / Fiabilitate Si Durabilitate*, (1), 206-212.

Sinanc D., Sagiroglu S. (2013). A Review on Cloud Security. *SIN '13 Proceedings of the 6th International Conference on Security of Information and Networks,* 321-325. doi:10.1145/2523514.2527013

Vaquero, L., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. *Computing*, *91*(1), 93-118. doi:10.1007/s00607-010-0140-x