David S. Li

Professor Stacey Suver

CSE 300

11/02/2017

Security Issues in Cloud Computing

In recent years, cloud computing has become increasingly utilized for personal and business usage. It has become an especially important tool for collaboration between users for working on projects, e.g. Still, despite its advantages, many potential companies, or clients, are reluctant to adapt the cloud model, out of fear of compromising what could be confidential data to a data breach, or even possibly to cloud providers themselves. Thus it is important to understand the security risks that persist with cloud computing, along with possible means to mitigate such risks.

Although cloud computing only became prevalent in more recent years, the history of the cloud actually goes back more than 40 years. J.C.R. Licklider introduced the Internet in the 1960s, but it wasn't until the 1990s that virtual private networks began to be used for data communication, when the "cloud" was first coined. Cloud computing continued to increase in popularity, when companies like Salesforce and AT&T quickly realized that they could provide their services through the web. Some of the most notable examples of cloud computing include Amazon Web Services and AT&T's USi, where application-based services for purposes like storage and computation are provided to clients. Today, it is used from a personal level to huge enterprises. Examples of it range from personal email to large scale data storage (Harauz 61).

With cloud computing, a provider is providing the services to be used by the client. This is done in multiple ways; Software as a Service, where the provider provides software and infrastructure so that the client can only run their software and use it on the cloud infrastructure, with no control over any underlying infrastructure; Platform as a Service, where clients can deploy software on the cloud infrastructure and modify any application settings as they please; and Infrastructure as a Service, clients are in full control of underlying infrastructure that they choose to deploy their software on. There are also four deployment models (public, private, community, and hybrid) that determine who a cloud infrastructure is accessible to, and five characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service) that determine how resources are provided to users (Aldossary 486). These concepts are important because they relate to how the provider controls how a client can use their cloud infrastructure and deploy software on it, along with who can access the infrastructure or software that was deployed. The above concepts determine essentially who can be subject to the cloud provider's authority, as will be discussed later.

Despite the many advantages that cloud computing has to offer, many are still turned away because of the security risks that are associated with it. The risks vary depending on the provider and the purpose of what clients may use a cloud infrastructure for. Especially when the user does not own the infrastructure for which they are deploying on, information that could potentially be confidential is being entrusted with cloud providers. Users are storing their data and software in remote locations that are owned by a third party. However, this exposes the risk of things like data breaches or hijacking happening to the potentially important data that is stored in these servers. Given a cloud can host so much data from so much users, measures must be taken to ensure its security; just one break-in can compromise the data of all users belonging to a

cloud, or the attacker may not necessarily compromise the data but deny access to that data (Aldossary 488). In order to give the customer a peace of mind, a service level agreement (SLA) must be kept to the highest possible standard. This SLA includes meeting required performance levels, proper management of any problems, and providing the necessary security to a user's information. In addition, the SLA should include provisions as to what happens, should a user's data be compromised in some way or the provider become acquired/cease to operate (Kandukuri 519).

There are means through which this situation could improve, although all differ depending on the possible type of situation that could affect a cloud computing infrastructure. Some suggestions that Minhaj Ahmad Khan makes in his survey of security issues for cloud computing include the use of frameworks, such as Mirage (Wei et al. (2009)) and PALM (Zhang et al. (2008)) to counter various types of virtual machine based attacks, since a huge portion of cloud deployments are in virtual environments (Khan 14). Other possible areas include intrusion detection and a secure execution environment. Currently, the most important things are being able to comply with federal regulations and being able to keep up with the rise of security issues. Complying with federal regulations is important because such regulations address issues such as privacy for health, financial, as well as encrypted information. At the same time, cybersecurity attacks have continued to be on the rise, and this is true for cloud infrastructures as well, so more countermeasures are needed to ensure that client data remains protected (Khan 25).

It is believed by Popovic in his publication that there is still room for improvement in terms of cloud security (Popovic 248). At the same time, the fact that security issues are on the rise when there are already measures in place brings into question the effectiveness of such measures. As such, it is becoming increasingly necessary to test the effectiveness of many

security measures, such as intrusion detection and even federal guidelines for protecting client data (Khan 26). While these measures may be well intended, as attacks on cloud servers increase we don't know for sure whether they, in their current state, are as effective as they are supposed to be. It is important for us to know what can be improved in terms of cloud security measures so that client data or applications can be better protected from attackers, whether this is a flaw in a regulation or in a framework designed to protect data/applications. Studying the effectiveness of cloud security measures can lead to better protection of client data and applications in the future. In a time where usage of the cloud is becoming more popular than ever, this would encourage more organizations to move data and applications into the cloud. In addition to increasing confidence in having organizations migrate to using cloud-based infrastructures, this would assist in the creation of future regulations or measures designed to help such users that store information in the cloud.

In addition to improving current security measures, we must also consider the future with regards to security. In particular, providers must continue to maintain trusted environments in the cloud for storing data and applications, where anything stored on the cloud must be in the best interests of the cloud provider and infrastructure. There are also issues such as protocol vulnerabilities and open standards compliance requirements. As regulations and models change, the cloud infrastructures will have to adapt to such changes. This means continually updating protocols to match these changes (Khan 26). This is also justification for evaluating current measures; even for those that are successful, it is necessary to determine if they will need to be changed, or if their success will hold in coming years. Again, this will help ensure that the cloud is a safer place for clients to store data and deploy their applications in.

The cloud has become a vital tool for storage of data, both for personal and business use alike. For large enough organizations and power users, it is even where complex applications can be deployed and tested. However, the prospect of using a remote server has led to concerns that such information can be compromised, whether through a security breach or a server failure. To combat such issues, there are security measures are in place to minimize data loss, whether on the provider's part or an attacker's part. However, with security issues on the rise as of late, many are starting to call into question the effectiveness of such measures. It is thus important to measure the effectiveness of security measures designed to protect cloud users and fix any issues found, even among those the measures that seem to be effective now. This will greatly improve cloud security and give users/clients a peace of mind in storing their data/applications in the cloud.

Works Cited

Aldossary, Sultan and William Allan. "Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions." *International Journal of Advanced Computer Science and Applications* (2016): 485-498.

Harauz, John and Lori M. Kaufman. "Data Security in the World of Cloud Computing." *It All Depends* (2009): 61-64.

Kandukuri, Balachandra Reddy, Ramakrishna Paturi and Atanu Rakshit. "Cloud Security Issues." *2009 IEEE International Conference on Services Computing*. 2009. 517-520.

Khan, Minjah Ahmad. "A survey of security issues for cloud computing." *Journal of Network and Computer Applications* (2016): 11-29.

Popovic, Kresimir and Zelkjo Hocenski. "Cloud Computing Security Issues and Challenges." *International Journal of Computer Networks* (2011): 247-255.