David S. Li

Dr. Suver

CSE 300 – Research Proposal

November 16, 2017

Improving Cloud Security Through a Survey of Current Issues

Cloud computing has undoubtedly become a vital business tool for deploying software and storing data. Yet the prospect of storing applications and data in a remote server arouses concerns, for data that is stored this way has the potential to be compromised, whether through an attack or through server failure. This is especially true for large organizations and businesses, which not only deploy big software programs on the cloud, but also store large amounts of data, possibly confidential, on these servers. Additionally, it poses a challenge financially to just store data and deploy software on these remote servers, and security flaws could result in drastic financial consequences for organizations. However, security issues also impact everyday home users on a significant level, as many have turned to the cloud to store work documents and back up personal, yet important items such as family photos. This research study is intended to focus on issues that have been discussed in recent literature, including but not limited to loose security measures and regulations for cloud users and providers, where it is unknown as to what steps should be taken to solve such issues. Hopefully, as a result of this study, there can be tighter regulations, such as improvements to current privacy measures that benefit clients.

In recent literature, researchers have pointed out that security measures exist to protect cloud users from compromising their data and applications, but organizations are still hesitant to migrate to the cloud because of deficiencies in these measures that have been pointed out.

Researchers have investigated several issues with regards to cloud security. Balachandra Reddy Kandukuri pointed out in his publication the holes currently present in Service Level Agreements (SLA's) designed to protect cloud users and their data, while defining rules that cloud providers are allowed to impose on their clients. He noted that SLA's need to satisfy basic requirements such as covering data loss not on the clients' part and being able to recover lost data in such situations. In addition, SLA's need to make additional provisions; because cloud servers are usually located in remote locations, so providers need to make clear where data will be stored in the event a client has reservations about their data being stored in specific locations; additionally, data is stored in the same servers as other users are using, so providers need to ensure as part of the SLA that user data is not shared with other users (Kandukuri 519). Sultan Aldossary, in his publication, identified virtualization as a potential security issue in cloud computing, as outsiders can attack a virtual machine (VM) or a VM image, causing problems such as data leakages, or even access a state of a VM that they are not supposed to have access to, leading to data potentially being compromised (Aldossary 491). Researcher Kresimir Popovic noted that just hosting data in the cloud can lead to increased costs for the organization (Popovic 253). The prospect of possibly losing data or software because of a security issue could potentially have serious financial implications for that organization. Despite researchers are trying to combat such security issues in cloud computing, the number of attacks has still continued to increase in recent years, and these statistics are only likely to worsen in coming years. In fact, most issues today are with regards to how cloud security should be increased in the long term to protect users (Khan 26).

Currently, it is unknown or vaguely known what direction researchers should go about solving many known issues to ensure cloud computing security in the long term. It has been

stated by Khan that there need to be improvements such as providing a trusted, secure environment for clients. However, it is not explicitly stated which improvements need to be made, and there is a loose definition of a "trusted environment"; it is also unknown what are the most important open standards to keep in mind when creating a cloud environment that conforms to such standards. This research study will survey the state of security issues that persist in various cloud servers. The subjects will be mainly servers that host large enterprises, as their use of the cloud is more significant economically. There will be variance based on factors such as geographic location, as researchers have pointed out that there are financial and security implications based on such factors. For this portion of my research, my plan is to evaluate several issues such as data loss and security attacks within a six month period and see whether they correlate with such factors. The test subjects will be evaluated based on strengths and weaknesses in their security measures. These strengths and weaknesses will be correlated with the amount of security issues that each subject has, in order to help determine the specific security issues that need to be addressed.

This study is intended to not just survey the current security issues that pose a threat to cloud computing, but also to evaluate trends between different cloud servers and how it affects the amount of security issues that they experience. The results of this study can have potentially significant implications; characteristics of cloud servers that are evaluated and deemed secure or insecure can guide providers towards being able to increase the security of their servers. Whereas it was unsure how providers should go about some of the issues identified in previous research, my hope is that as a result of this study cloud providers will have some idea as to how to address many of these issues. In addition, this study will hopefully extend our understanding as to what may have been behind prevalent issues in cloud security.

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.