The Use and Advantages of Cloud Computing

(Technical Paper)

The Future of Cloud Computing and the Risks It Holds

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Kiyan Zewer

Fall, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

STS Advisor: Richard D. Jacques, Ph.D., Department of Engineering & Society

Introduction

Cloud computing has become an essential tool of everyday life as it continues to grow as a powerhouse of data. The cloud is a server that is accessed through the internet to host databases and software for various purposes. This information could then be manipulated to learn more about the cloud and its use. This process is known as cloud computing. The use of cloud computing offers various perks such as lower cost, speed, global scale, productivity, performance, and reliability (Azure, 2022).

My technical part will be about my internship experience from this past summer. I worked as a cloud engineering analyst where I evaluated the usage of the cloud to maximize efficiency and cost. I created plots of users' cloud data to represent their cost and usage over a set period. Throughout this experience, the risks of the cloud through cloud computing were evident and more questions began to arise about the security surrounding cloud computing.

While cloud computing has advanced the technology industry, some disadvantages are seen as possible risks. My STS research will focus on the reliance on cloud computing, security risks, and the overall outlook in the future. Essentially, my research question is about all aspects of security within cloud computing, including data exposure recovery, data loss, and much more. Given the huge shift of data being saved within the cloud, there needs to be a process to ensure the security of such vulnerable data.

Technical Discussion - The Use and Advantages of Cloud Computing

The use of cloud computing rids the need for the capital expense of hardware and software for data centers. A key feature includes easy access to the data to decrease the time it takes to get to the information. Cloud computing can efficiently scale so that the proper amount of computing power, storage, and bandwidth is used when needed. There is no longer the need to

set up hardware as the cloud systems are all within the internet, which allows for more time allocated to other tasks.

A benefit of cloud computing includes reduced network latency for software (Azure, 2022). The data centers are constantly updated and upgraded to sustain their usage. Salesforce's article, "12 benefits of cloud computing and its advantages", highlights the reliability of cloud computing and how it is essential as it can back up and recover data readily. Companies must prepare for a disaster as it can occur in a multitude of manners. While all disasters cannot be prevented, their recovery process can be sped up. Only 9% of non-cloud users claimed that their disaster recovery was within four hours or less, whereas 20% of cloud users claimed they could (Salesforce). Salesforce held a survey where they saw that 43% of IT executives claimed they would invest in a cloud-based disaster recovery plan. While cloud computing can prepare for unexpected issues, it can also work to prevent them. If cloud computing is not used to store data, all the data will rely on the local hardware of the computer. In the case that anything was to happen to the computer, whether it be a virus or a physical malfunction, then the data will be lost and no longer recoverable. However, cloud computing provides a backup option for storing data that can be resorted when necessary.

Scalability within cloud computing incorporates the ability to increase or decrease IT resources. Companies have various requirements depending on the number of employees. The cloud allows companies to quickly scale up and down their IT departments. Scalable cloud architectures are created through virtualization. Virtual machines are flexible, easily scalable, and can be moved to different servers or be on multiple at once. A virtual machine is a resource that uses software instead of physical hardware to run programs and act as a computer (VMware, 2022).

My internship was an example of the many advantages of the cloud. I could immediately grab data and parse it freely through many applications. For example, I pulled all the cloud data from a user's account as an excel and imported it into a Jupyter Notebook. This notebook then allowed me to use the programming language Python to create plots to display the data I acquired. I created plots to show the cloud spending by the user over a given period. This would show trends such as spending on weekdays against weekends, spending on various apps, and much more. I could then use Facebook Prophet, a Python library, to forecast future spending so that users could see what their spending could look like in the future based on previous patterns.

Through my experience, I encountered many of the perks of cloud computing. I could see how a cloud could host a database. The ease of accessing the data was as easy as clicking a few buttons in a matter of seconds. I was left curious if this data was exposed due to the ease of access. However, to keep this data secure, there are many layers of security, including encryption, two-factor authentication, and ongoing monitoring. Data recovery was extraordinarily useful as data loss was seen quite frequently. Fortunately, a simple backup could restore the lost data as the previous work was kept on the server. Scalability was present as I could access the cloud whether it was on my personal laptop, work laptop, or in the office. The cloud has created an efficient method of storing data that shows why it is growing at a rapid rate.

STS Discussion - The Future and Risks of Cloud Computing

Five common security issues unique to cloud computing include unauthorized access, reduced visibility and control, unsecure APIs and interfaces, system vulnerabilities, and data breaches, loss, or leakage (Antonenko, 2021). Creating ease of access to data has the potential risk of unauthorized access. Organizations are exposed when services are used without their knowledge. Employees having access to hosted data from remote services could inject external

security threats. If the employees were to have a lapse in security, then there could be a breach in the data center.

As an organization shifts to a cloud-based data center, there will be a lack of visibility and control. The cloud provider becomes responsible for the policies and infrastructure of the data center. Cloud data protection issues can be caused by improper handling by the provider. This would reduce the effectiveness of security that is supposedly ensured by the cloud.

Application Programming Interfaces (API) are a fundamental aspect of the cloud experience. APIs allow enterprises to use techniques such as encryption to protect the data. However, APIs can also pose a threat to the security of the cloud if designed poorly as they can allow an attacker to use methods, such as decryption, to gain access. Hackers working for the Kremlin targeted a popularly used Microsoft cloud service and compromised cloud identity systems (Herr, 2021). They could then steal certificates to create their own identities to gain access to Office 365 accounts and impact thousands of users. Similarly, unsafe operating systems, shared memories, and other system vulnerabilities are seen as gateways to data thefts. These are points of entry to malicious attacks as the system becomes vulnerable through exploitable bugs giving leverage to confidential information. For example, in 2019, there was a breach at Capital One, an Amazon Web Services (AWS) cloud user (Herr, 2021). The combination of the AWS cloud vulnerability and Capital One's struggle to configure a complex cloud service led to a data breach of tens of millions of customer records.

While there have been liabilities of cloud usage, there have also been responses to overcome these risks. To mitigate these risks, there would need to be an incident response plan to identify and properly respond to unconventional behavior. Norton's (2022) article, "Cloud Security: How Secure Is Cloud Data?", explains that cloud security is seen to be far more robust

now due to artificial intelligence (AI) tools, security updates, built-in firewalls, backed-up data, and third-party security testing.

Trends are showing that cloud computing is building a mutually beneficial relationship with artificial intelligence (Tech Journal, 2022). Cloud computing services are used as a form of advertisement to enterprises to persuade them to use AI-enhanced packages. AI and machine learning have been used to increase the safety of cloud systems to create automation of monitoring attacks and defense processes. These programs use built-in algorithms to expose vulnerabilities to the user.

Security updates are an effective method for updating operating systems to protect devices from viruses and malware that can pose a threat. Cloud providers also apply firewalls to monitor incoming traffic. The firewall instills specific rules to keep the cloud secure as it makes it more difficult for attackers to inject malicious code. Backed-up data is an automated process of copying data several times and having it stored across multiple data centers. This is effective in the case that data is lost or if the server is inaccessible, as the files would still be accessible on the backup server. For example, on July 17th, 2020, the company “Cloudflare” was responsible for the shutdown of nearly half of the internet (Abdullah, 2020). This was due to their server having an issue and not being operational. Fortunately, the Cloudflare team could act quickly and use their backup server as a host as they solved the issue. However, this presented the issue that there is an abundance of dependency on the cloud being operational.

The future of cloud computing in 2030 is predicted to be worth approximately $1,620,597 million (Tech Journal, 2022). Based on a 2019 estimate of $325,689 million, this is 16% compounded annual growth. Convenience and usage are the key reasons that businesses have shifted to a cloud network. It has been especially dominant after the pandemic as companies

seek new methods of using the cloud in a remote setting. The continuous growth of the audience inspires the growth of the cloud.

Conclusion

The cloud has grown as a part of our everyday life through video streaming platforms, file hosting services, secure storage of personal data, backup solutions, and even chatbots (CriticalCase, 2022). The goal of this project was to look at the evolution of cloud computing as a tool. Originally, through my internship, I had first-hand experience with how cloud computing could revolutionize the technology industry. These also raise questions about the security of cloud computing.

Through research, the disadvantages of cloud computing were evident as there were security concerns. This was due to the original lack of preparation and defense against external factors. Over time, the necessary security adaptations have been made and created a secure environment that businesses are shifting toward. These changes have created a form of trust between users and the cloud that allows it to become an imperative prospect of the technological world.

Word Count: 1773

References

Abdullah. “Cloudflare Crashes: Discord, Patreon and Hundreds of Websites Unavailable.” *Gizchina.com*, 18 July 2020, www.gizchina.com/2020/07/18/cloudflare-crashes-discord-patreon-and-hundreds-of-websites-unavailable/. Accessed 25 Sept. 2022.

Antonenko, Dimitri. “Cloud Computing Security Issues and Challenges - Businesstechweekly.com.” *Businesstechweekly*, 4 Jan. 2021, www.businesstechweekly.com/cybersecurity/data-security/cloud-computing-security-issues-and-challenges/.

Azure. “What Is Cloud Computing? A Beginner’s Guide | Microsoft Azure.” *Azure.microsoft.com*, azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits.

CriticalCase. (2021, July 26). *5 practical use cases of cloud computing in Everyday Life*. Criticalcase. Retrieved October 31, 2022, from https://www.criticalcase.com/blog/5-practical-use-cases-of-cloud-computing-in-everyday-life.html

Globaldots, A. (2022, September 12). *13 benefits of cloud computing for your business*. GlobalDots. Retrieved October 30, 2022, from https://www.globaldots.com/resources/blog/cloud-computing-benefits-7-key-advantages-for-your-business/

Herr, Bruce Schneier, Trey. “Russia’s Hacking Success Shows How Vulnerable the Cloud Is.” *Foreign Policy*, foreignpolicy.com/2021/05/24/cybersecurity-cyberattack-russia-hackers-cloud-sunburst-microsoft-office-365-data-leak/.

Norton. “Cloud Security: How Secure Is Cloud Data?” *Us.norton.com*, us.norton.com/blog/privacy/cloud-data-security. Accessed 25 Sept. 2022.

Salesforce. (n.d.). *12 benefits of cloud computing and its advantages*. Salesforce.com. Retrieved October 30, 2022, from https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/

TechJournal. (2022, October 12). *What is the future of Cloud computing 2025?* Tech Journal. Retrieved October 31, 2022, from https://techjournal.org/the-future-of-cloud-computing-2025/

Techjournal. “What Is the Future of Cloud Computing 2025?” *Techjournal*, 9 Mar. 2022, techjournal.org/the-future-of-cloud-computing-2025/.

VMware. (2022, October 19). *What is a virtual machine?: Vmware glossary*. VMware. Retrieved October 30, 2022, from https://www.vmware.com/topics/glossary/content/virtual-machine.html

VMware. (2022, October 19). *What is cloud scalability?: Cloud scale*. VMware. Retrieved October 30, 2022, from https://www.vmware.com/topics/glossary/content/cloud-scalability.html#:~:text=Cloud%20scalability%20in%20cloud%20computing,its%20exploding%20popularity%20with%20businesses.