Cloud Computing and its Cybersecurity Concerns

California State Polytechnic University, Pomona

by

Jackie Fortner

Mayela Ancheta

Jessica Pinto

Alice Nguyen

CS2610: Introduction to Cyber Security and Network Communication

Professor Danica Cariaga

December 2023

Abstract:

This paper delves into the multifaceted aspect of cloud computing, exploring its definition, working mechanisms, real-world applications, and the pivotal role it plays in modern business operations. A significant focus is placed on the critical facet of cybersecurity, addressing vulnerabilities, their potential exploitation, safeguards, and emerging trends of cloud security.

1. Introduction

Cloud computing involves the delivery of computing services (such as storage, processing power, and applications) over the Internet. It eliminates the need for organizations to invest in and maintain physical infrastructure, allowing them to scale resources dynamically. Organizations worldwide are swiftly adopting cloud services due to their cost-effectiveness, scalability, and flexibility. This widespread adoption underscores the critical role of cloud computing in modern business operations. As businesses entrust sensitive data to cloud providers, ensuring robust cybersecurity measures becomes paramount. The interconnected nature of cloud environments necessitates a comprehensive approach to safeguarding data, applications, and infrastructure. In the digital era, cloud computing is a revolutionary paradigm that uses the Internet to offer computer services, reinventing resource scalability and doing away with the need for physical infrastructure. Robust cybersecurity measures are becoming increasingly important as organizations all over the world adopt cloud services to safeguard critical data, apps, and infrastructure.

2. What is the Cloud?

Cloud computing refers to the “use of hosted services, such as data storage, servers, databases, networking, and software over the Internet. The data is stored on physical servers, which are maintained by a cloud service provider. Computer system resources, especially data storage and computing power, are available on-demand, without direct management by the user in cloud computing" (Patil, BasuMallick, 2022). The Cloud allows users to store files and data on the cloud, rather than on a storage device or hard drive, and this allows them to access the files from anywhere with an internet connection.

3. How does it work?

"The Cloud can be divided into two different layers, namely, front-end and back-end" (Patil, BasuMallick, 2022). Users interact with the front-end layer, enabling them to access the data they have stored in the cloud. On the other hand, the back-end layer is, then, the software, hardware, servers, etc. This layer is the "primary component of the cloud and is entirely responsible for storing information securely. To ensure seamless connectivity between devices linked via cloud computing, the central servers use a software called *middleware* that acts as a bridge between the databases and applications" (Patil, BasuMallick, 2022). Furthermore, to maintain availability, cloud providers typically spread data to multiple virtual machines in data centers around the world. If more storage is required, the cloud provider will initiate more virtual machines.

4. Brief History

As stated, cloud computing was revolutionary to organizations across the globe, however even before its debut the concept of computing as a utility or service wasn't necessarily new. During the year 1965, the development of minicomputers came along, though they were only accessible to extremely wealthy corporations at this time. Around the same time, John McCarthy invented time-sharing which was an operating system that allowed multiple users to have access at the same time to a large and powerful mainframe computer that was shared through remote terminals. The rise of time-sharing made the developing idea of cloud computing accessible to a large number of companies due to its affordability. With an ever growing demand for data processing necessities of smaller companies, the time-sharing business experienced a huge growth birthing over 100 time-sharing companies. The rise of PCs and Unix workstations quickly ceased the existence of those companies bringing about huge modern data centers..

During the year 1999, VM (Virtual Machine) technology was reinvented for x86 systems providing a foundation for cloud computing services as we know it. Shortly after this innovation early cloud services were introduced such as; VPNs, network file shares, application containers, etc. Though the exact year in which cloud computing was invented is hard to trace back to due to its continuous developments from the late 1990s to early 2000s, the breakthroughs that eventually brought about modern cloud computing can be dated. Following the use of time-sharing, Application service providers (ASPs) and consumer information services, the installation of larger internet circuits and the idea of remotely executed applications were adopted by a growing number of organizations creating a revenue explosion within the industry.

The evolution of cloud computing is intricately intertwined with the surge of e-commerce during the early 21st century. Major online organizations such as Amazon, Google, and Microsoft played pivotal roles in this transformative journey by establishing massive data centers to cater to the skyrocketing demands of online commerce and applications. As these companies sought efficient ways to handle the growing volume of data and provide scalable services, the concept of cloud computing emerged as a solution. The pivotal moment came in August 2006, during an industry conference, when Google CEO Eric Schmidt introduced the term "cloud" to describe this shift in computing. This marked a turning point, and within the same year, its widespread use took off with Amazon's launch of Amazon Web Services (AWS), featuring the

Elastic Compute Cloud (EC2). Which not only marked the inception of widely adopted cloud services but also laid the foundation for a revolutionary approach to computing that broke traditional boundaries paving the way for the diverse cloud ecosystem we are fortunate enough to know today.

5. Real-world Applications

In our modern age, cloud computing services can practically be found across every industry sector (Healthcare, Education, Government, etc.) However, this goes beyond mere cloud storage services that are more likely to come to mind.

For example, a large number of hospitals have implemented cloud computing within their facilities granting the patient access to their medical record anywhere and anytime they desire. Before, if someone wanted to know specific information found on their medical file they would have to call their designated clinic and request that information. This could be a frustrating process for both parties; for starters, the clinic had to cautiously verify the person's identity due to HIPAA policies in place which are in place to protect a patient's sensitive health information. After doing so, the clinic had to search for the file and either send the information over or have the patient pick it up. Now, with a combination of cloud computing services and authentication methods this process can be completed in one's fingertips within a few minutes. A patient logs into a designated app or website with their personal username and password and are authenticated completing the verification process. After that they are free to see their up-to-date test results, specific conditions and/or prescriptions. Cloud computing has facilitated the lives of many across the globe by increasing accessibility to one's own health information

Another example can be seen daily within classrooms with software such as Canvas or Google Classroom. Most schools K-12, extending all the way through secondary education have adopted these applications or similar ones which grant students unlimited access to their course material. The developments made by these applications through the use of cloud services has provided a better learning ecosystem for students worldwide. It’s broadened the learning scope immensely with its power by expanding the horizons of learning as we traditionally knew it. Without failing to mention the cost efficiency of it all, on printing materials alone schools have seen billion dollar decreases within their annual expenditures. Prior to such applications, teachers would have to print all course material in order to give students access to it. Now, an instructor can upload assignments, projects, instructions, quizzes etc. to the cloud and in that same instant the students will have access to it on their side. Additionally, thanks to this innovative technology both students and instructors don’t have to carry around heavy back-pain causing backpacks that contain textbooks, assignment packets, etc. Such programs require minimal hardware, a student could even access their desired material from their phones if necessary. On a larger scale, schools themselves can transfer their data to an off-campus cloud server which also significantly reduces their storage costs and guarantees adherence to the strict security measures set in place through FERPA.

An additional example can be seen within the United States government, during the Obama administration the US Federal Cloud Computing Strategy was introduced making both the government and military early adopters of cloud computing services. Though the process was a lot more tedious when it came to transferring data as there are various strict compliances and security measures the sector must adhere to due to widely feared domestic and/or foreign attacks. One huge pro to cloud computing within the military is its contribution to collaboration and communications. Cloud tools have granted secure communication among military personnel no matter where they’re stationed around the world. Crucial files containing necessary tactics and/or strategies can now be easily but most importantly securely shared among different branches vastly improving overall coordination. Another benefit is how efficient cloud security analytic tools help to identify cyber threats allowing the government to counter-attack these threats before they continue to grow. Such threat intelligence has allowed the military to share these identified threats in real time greatly improving their defense systems. These are only a few examples of how cloud computing has significantly enhanced various aspects of the US government.

As a whole we can see that cloud computing services have been able to strengthen various kinds of industry sectors from data management to cybersecurity. The widespread use of cloud technology has granted flexibility, efficiency and scalability in meeting the complex standards the real world demands.

6. Importance to Cybersecurity

As the cloud becomes a more prominent tool, cybersecurity is especially important to protect users' and company data. Security threats have become more advanced as the digital landscape continues to evolve and hence, countermeasures must evolve alongside them. Furthermore, due to the importance of the information that is stored on the cloud, it is very important that all the data is kept secure. Not only that but it must also be taken into consideration the amount of information that is stored on the cloud. Whether it be from Amazon, Apple, or Google, the cloud is an almost universal resource when it comes to technology. An attack on cloud security could prove detrimental to people all over the world, with potential consequences hitting entire countries at a time, even if not intended. While governments, mega-corporations, and major organizations use their own secure cloud services, it is still vitally important to implement security measures to ensure the safety of the information stored on these services. Additionally, "these threats explicitly target cloud computing providers due to an organization’s overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information” (Google).

7. Cloud Security

“Cloud security refers to the cybersecurity policies, best practices, controls and technologies used to secure applications, data, and infrastructure in cloud environments” from the many possible internal and external threats that exist (Google). That said, cloud security challenges must be combatted and some of these include: lack of visibility, compliance, multitenancy, misconfigurations, and access management, to name a few. Multitenancy refers to when “public cloud environments house multiple client infrastructures under the same umbrella, so it’s possible your hosted services can get compromised by malicious attackers as collateral damage when targeting other businesses” (IBM). Moreover, access management refers to the property when “cloud deployments can be accessed directly using the public internet, which enables convenient access from any location/device. This also means that attackers can more easily gain authorized resources with compromised credentials or improper access control” (Google). Furthermore, as mentioned, misconfigurations are a key component to monitor for in cloud security. Such an instance is when cloud settings are misconfigured leaving the potential for data breaches. Such mismanagement leads to vulnerabilities and it is hence important that those dealing with the infrastructure of the cloud be well versed and knowledgeable of the technology.

8. Exploitation and Safeguards

With the volume and vitality of the information stored on the cloud come malicious outsiders seeking to manipulate or gain access to such information. A multitude of exploitative paths and methods exist, all of which will be elaborated on further but include a combination of misconfigurations, lack of visibility, poor access management, insider threats, unsecured APIs, Zero-Days, Shadow IT, and lack of encryption. Misconfigurations can be a source of exploitations since attackers use misconfigurations in cloud settings to enter into the cloud database. In 2022, McGraw Hill was susceptible to a misconfiguration exploit that left the grades of university students all over North America open and available for the public to see. Working with the cloud, it is impossible to fully implement an effective security system without visibility of the entire cloud ecosystem, an issue that makes all other present vulnerabilities easy to reach for attackers. Through lack of visibility, the Japanese car company Toyota became susceptible to a data breach that revealed the car location information of 2.15 million customers for nearly 10 years. The most pressing issue with this case is the timeline, considering the breach occurred in November 2013 and is reported to have concluded in April 2023. Moving on to the next vulnerability, insider threats are often magnified in cloud environments, largely due to the fact that cloud based applications can be accessed from unsecured devices or by using unsecured APIs. Time and again, insider threats work hand in hand with poor access management, which is simply a lack of security measures. Businesses with poor access management tend to lack critical, straightforward measures such as employees using secure passwords and limits on employee resources or authorization. Zero-day is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. Essentially, if a vendor or developer has only just learned of a flaw, they have ‘zero-days’ to fix it, hence the name. Finally, Shadow IT relates to the use of IT related hardware or software by a department or individual without the knowledge of the IT or security group within the organization. All these factors contribute largely to the vulnerability of cloud computing, however it is possible to establish safeguards to prevent or at least minimize the consequences of a breach. In terms of exploitation through misconfigurations, it is suggested to implement least privilege access to cloud resources and use cloud security posture management. To reduce lack of visibility, implement centralized logging and monitoring solutions for all cloud resources. Many small businesses install security scripts on their websites to protect against known threats and vulnerabilities, however these scripts are unable to access many third party components since they are limited by browsing restrictions. A more general list of potential safeguards for information on the cloud with potential vulnerabilities include external or installed monitoring, enhanced visibility (which can be achieved with external monitoring), and maintaining extremely tight security against third-party scripts.

9. Future Trends in Cloud Security

The landscape of cloud security is dynamic and constantly evolving in response to emerging threats and technological advancements. As organizations navigate an increasingly complex digital environment, it becomes imperative to anticipate future challenges and proactively adopt strategies that align with the evolving nature of cyber threats. One prominent trend is the continual evolution of the threat landscape, marked by the emergence of sophisticated attack vectors such as zero-day vulnerabilities and advanced persistent threats (APTs). Recognizing and understanding these evolving threats is essential for organizations to prepare and fortify their defenses. Moreover, the integration of cutting-edge technologies is becoming pivotal in enhancing the resilience of cloud security. Artificial intelligence (AI) and machine learning (ML) are progressively being harnessed to augment the ability to detect and respond to cyber threats in real time. These technologies offer the promise of predictive analytics, enabling security systems to identify patterns indicative of potential threats before they materialize. Staying abreast of these technological advancements is key to maintaining robust security in the cloud. As cloud computing continues to be an integral part of modern business operations, the adoption of these trends not only safeguards against current threats but also lays the foundation for a proactive and adaptive security posture in the years to come.

10. Conclusion

In the primarily digital society of today, cloud computing has grown to become a part of almost every other technological service provided on and off the web. From home security systems to corporate databases, it is used across a variety of platforms and trusted worldwide. Different layers of cloud computing exist and the connection between application and data is the key feature of the service, allowing it to be a source of dynamic memory for large amounts of data that can be obtained with little to no delay. However, with the volume of data stored on the cloud, it is imperative that security services remain up to date and vulnerabilities are identified and amended promptly. While there are a myriad of vulnerabilities throughout cloud computing, there are an equal number of safeguards that can be put in place to significantly reduce the damage an attack could produce. No system can be completely secure, yet systems like the cloud are used by millions around the world. As cloud computing evolves, it will continue to present new vulnerabilities and call for many more safeguards, and with new technologies like artificial intelligence and machine learning, the sky is the limit when it comes to the cloud.

Works Cited

NIST Special Publication 800-145: “The NIST Definition of Cloud Computing” - National Institute of Standards and Technology (NIST). NIST Cloud Computing Definition.

Patil, P., & BasuMallick, C. (2022, February 9). What is cloud computing? definition, benefits, types, and Trends. Spiceworks.

Velazquez, R. (2022, September 12). Cloud computing. What Is Cloud Computing? How the Cloud Works. Built In.

"8 All-Too-Common Cloud Vulnerabilities." Wiz.io, 7 Sept. 2023, www.wiz.io/academy/common-cloud-vulnerabilities.

Kaspersky. “What Is a Zero-Day Attack? - Definition and Explanation.” *Usa.Kaspersky.Com*, 30 June 2023, usa.kaspersky.com/resource-center/definitions/zero-day-exploit.

“Lack of Visibility: The Challenge of Protecting Websites from Third-Party Scripts.” *The Hacker News*, 5 May 2023, thehackernews.com/2023/05/lack-of-visibility-challenge-of.html.

"5 Real-World Examples of Cloud Computing." Maropost | The Unified Platform Designed to Drive Growth, 7 June 2022, www.maropost.com/5-real-world-examples-of-cloud-computing/.

"Decoding the Cloud Computing Timeline." Atos, 14 Apr. 2023, atos.net/en/blog/decoding-the-cloud-computing-timeline.

"The History of Cloud Computing Explained." WhatIs.com, www.techtarget.com/whatis/feature/The-history-of-cloud-computing-explained.