Shad Kamil Gafoor

IT 104-001

Tuesday, November 14, 2023

The Development of Cloud Data

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://catalog.gmu.edu/policies/honor-code-system/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ web site.

Introduction

Cloud data is an integrated data management system that gives people an internet-accessible remote server where multiple people can access storage from different devices, this creates wider availability for data and centralizes storage. The Cloud first began saw serious expansion in the early 2000s with Software-as-a-Service (SaaS) (Maayan, 2021) and a standard encryption algorithm called Data Encryption Standard (DES) (Alemami et al., 2023), but still has concerns that need to be addressed. This paper will go over the history of Cloud storage and its current and future developments, as well as its legal, social, ethical, and security concerns; with researched and emerging systems to mitigate them.

Background

Data systems resembling the Cloud were developed by computer scientist J. C. R. Licklider with the Advanced Research Projects Agency Network, (ARPANET), that allowed people to share data between computers. Cloud usage increases in the 1990s with Salesforce operating their software-as-a-service (SaaS) on Internet Cloud storage. SaaS being a licensed storage system from a service provider on a subscription. The 2000s saw many major tech companies switching over a large portion of their data storage to the Cloud: Google creating Drive, Amazon with Amazon Web Services, and in 2011 Apple released the iCloud. A multitude of independent tech startups were founded centered around Cloud storage, (Maayan, 2021). One prerequisite for operating a Cloud server is access to the internet, because the Cloud operates on a virtual server. These servers can come in many forms, depending on how centralized and private an organization desires: Public Clouds are ones provided by an external provider and can

be accessible by many individuals and organizations, Private Clouds are ones specifically provided by and for a single organization, while Hybrid Clouds still require on-premises servers but still having internet access to storage, (Rhoton, 2009).

Potential Benefits

Cloud data storage has generated more accessibility for people across organizations for data and collaboration, and with organizations able to open their Cloud storage to outside individuals giving access to more data for research or education on public storage. This accessibility is also granted on multiple devices since most Cloud storage does not require external hardware, allowing for multiple individuals to collaborate on the same project, (Rhoton, 2009). The advantage in concentration out of large physical data servers makes applications cheaper than previous storage systems (Alemami et al., 2023). These are offered by third party service providers, most commonly by SaaS storage, that lifts the burden of cost and on-site facilities. Online storage also creates the capacity for more storage than physical servers, and because of the cheaper prices, more companies and organizations are seen making the transition to Cloud storage. This system can also be properly scaled based on the operations and size of an organization

Security Concerns

The shift from mostly single device storage units and large server rooms to internet Cloud data has concentrated data access and made a more data accessible for single data hijacking attacks. Companies and organizations are required to have higher security measures to protect data for their users. A kind of concentrated attack is a Denial-of-Service attack, where a

malefactor denies access of the Cloud server to its intended individuals, (Rhoton, 2009). Data concentration and movement away from regulated supervision increases the risks of Data theft and leakages, and ultimately the cracking of DES security by hijackers, now considering it an outdated encryption code (Alemami et al., 2023). However, an investigation into different varieties of Cloud data encryption was done by Alemami and other researchers in a study to determine the security, data encipherment capacity, memory usage, and encipherment of various varieties. They found that Advanced Data Encryption (AES) had the highest capacity of data encryption and takes the least amount of time to encipher data. This was because of AES's block cipher, which encrypts a large block of data protected by a symmetric key to access any block that is randomly generated by a complex algorithm that is noted to be undecipherable by a majority of brute-force methods. However, this is tough to implement for many companies and organizations because of its size and complexity and is mostly used by government institutions. Another effective encryption algorithm was Blowfish which is similar to AES in that it uses a symmetric block cipher but with a less complex algorithm and slightly smaller capacity for data encryption but is still one of the fastest algorithms and is in the public domain, making it a popular encryption model for companies and organizations.

Legal and Ethical Issues

Cloud data has allowed for more people to work remotely from a wide array of jobs and organizations, allowing for people to be more productive and have more time to themselves. But there are some companies that prefer to have workers together in offices to create a spirit of unity and more easily concentrate directions, but workers now know that companies would be

unreasonable to force them not work remotely. Companies must find a balance between remote work powered by the Cloud and in person work to create an effective administration between data and people (Rhoton, 2009). Cloud service providers manage data storage for companies and organizations, and there are times when organizations have no say or information regarding how the data is stored but are still held liable if there are data breaches, and so are required to research service providers that are reliable in keeping their Cloud storage systems secure (Brady, 2010). Service providers are also capable of becoming unresponsive to companies and organizations or ending service abruptly, particularly with smaller ones. Forcing smaller companies to face the consequences of a sudden loss of storage and rallying lawyers in an attempt to mitigate these practices (White, 2010).

Social Problems

Because of the data sharing and accessibility aspects of Cloud storage, data privacy can be an issue for individuals uploading onto the same Cloud, particularly for Public Cloud storage. Because people with access to the Cloud can freely access any data not behind a clearance wall, it becomes a priority for administrators and service providers to create a system that only allows certain individuals or organizations to have access to certain areas of the Cloud for confidential data (Maayan, 2021). There can also be a problem of service providers being unwilling or unresponsive to cooperate with organizations to operate on a more private level and mostly leaves smaller organizations with the risks of Cloud storage (White, 2010). There is also a lack of customizability with SaaS service providers limiting organizations and individuals to a predetermined system that may not actually be the best fit for them, which also shows how third-

party service providers have more control over certain organizations' data storage than actual organizations. This control covers both software and governance of the data in a way that also creates what is known as Service provider Lock-ins, where data may not be portable from for cost or technical reasons from one service provider to another thus locking in a company or organization with a certain service provider (Watts et Raza, 2019).

Future Research and Usage

Cloud data storage is projected to continue growing, with new innovations like Infrastructure-as-a-Service (IaaS) that are projected to overtake SaaS in the fastest growing Cloud data storage system in the coming decades that will give individuals and organizations more control and security when it comes to their storage (Watts et Raza, 2019), which allows for greater virtual storage. Along with MultiCloud storage, with a organization utilizing multiple public Cloud service providers on a single Cloud network. This mitigates concerns about certain providers using Lock-in tactics on organizations and, when managed properly, a more flexible system for storing the same amount of data on terms that an organization has more control over (Maayan, 2021). And as more research and development is put into the more advanced data encryption algorithms and codes, like AES and Blowfish, it will allow them to become more accessible for mor companies and organizations that would create extra layers of safety for their data and individuals (Alemami et al., 2019).

Conclusion

Cloud data storage is still a developing field that has proven to have the potential of bringing more accessibility to its users, whether just individuals or entire organizations and companies. Cloud storage is also projected to be the majority or data storage systems in a couple of decades and thus would be the target of a larger amount of attempted data breaches and Denial-of-Service attacks, but with knowledge on research into more secure data encryption methods, companies and organizations and find a system that is highly secure, like AES, but still affordable and applicable, like Blowfish encryption. And as companies and organizations become more aware of these systems, they can apply them in a setting where they analyze different Cloud service providers on their integrity and reliability of vendors and avoid of ones that practice Lock-in systems or have an inflexible or uncompromising system that could be instantly implemented in a software update. MultiCloud systems are an emerging way of mitigating this, by using multiple service providers that may complement each other in terms of security and practice.

References

Alemami, Y., Al-Ghonmein, A., Al-Moghrabi, K., & Mohamad, A. M. (2023). Cloud data security and various cryptographic algorithms. *International Journal of Electrical and Computer Engineering, 13*(2), 1867-1879. https://doi.org/10.11591/ijece.v13i2.pp1867-1879 Accessed September 3, 2023.

The people behind this research paper are well learned computer scientists and professors. This source speaks briefly about how Cloud storage algorithms and codes have become more popular recently and the methods are varied. They analyze many different varieties of Cloud encryption and algorithms to determine how secure each of them is. The algorithms are in comparison of each other and how well they encrypt data and how fast, to also their complexity and storage capacity. This is important for the benefits of well-developed security measures and the social issues that would come from not having properly protected Clouds for organizations and employees at risk of having data stolen or naturally erased.

Maayan, G. D. (2023, April 13). *How the Cloud has evolved over the past 10 years*. DATAVERSITY. https://www.dataversity.net/how-the-Cloud-has-evolved-over-the-past-10-years/. Accessed September 3, 2023x

Gilad David Maayan is a technology writer on Dataversity and a 3-time winner of international technical communication awards for his work. This website paper describes the history of the Cloud Storage System as it developed through the internet and how data is stored

on independent networks. It goes further into how multiple companies in the early 2000s were pioneering this technology and the social benefits it provided for people who could work remotely and how it is developing today. Then finishes with growing methods of storage like Infrastructure-as-a-Service and the MultiCloud services.

Rhoton, J. (2009). *Cloud computing explained implementation handbook for enterprises* (2nd ed.). Recursive Press. Accessed September 19, 2023.

John Rhoton is well established Computer Science specialist and has been a strategist for Cloud Computing and other developments for companies like Microsoft and forums like the HP Technology Forum. This book covers the basics of what cloud computing is and the various storage services provided. He goes into detail about Public, Private, and Hybrid services and the expanse of Cloud Computing. He gives recommendations on what organizations are best suited to each type and how to assess providers. While not all of his information was utilized for this paper, he has a comprehensible style of writing that makes it easy to digest. The IT landscape has been changed by Rhoton's work and has been influential on this paper.

Brady, K. (2010, December). Cloud Computing—Panacea or Ethical "Black Hole" for Lawyers (The Bencher—November/December 2010). American Inns of Court., http://www.innsofcourt.org/Content/Default.aspx?Id=5499. Accessed September 21, 2023

Kevin Brady is a well-educated figure currently working on the Corporate Counsel E-Discovery RIM of Volkswagen of America. He received his Master's in Business Administration as well as being a Juris Doctor from Widener University. His article was cited here from *The*

Bencher, the publication of The American Inns of Court, its features are written by experts with "central themes such as legal ethics, professionalism, civility, or mentoring." His article was written for the purpose of expressing the legal and ethical concerns that lawyers and businesses should be aware of when dealing with cloud technology.

White, R. (2010, August 24). Cloud Computing: Advantages and Disadvantages | The Boardroom Brief Blog. Gunster's Boardroom Brief., http://boardroombrief.com/theblog/2010/08/24/Cloud-computing-advantages-and-disadvantages/. Accessed September 21, 2023

Robert White is a lawyer with many years working as a consultant to firms when it comes to dealings with service providers and in 2007 was, as one of the "Best Lawyers in America" for corporate and technology law. His article goes over the potential benefits of Cloud computing for businesses and entrepreneurs but also goes over risks. For the purposes of this paper, he was primarily used for the risks associated with legality of certain practices and for privacy concerns. He notes that third party service providers do not provide full information about their practices and policies and warns organizations about how they will have little control over the data storage and encryption. He recommends organizations make contingency plans based on the practices of the service providers. For legal protections re recommends organizations have a clear written form of what the relationship between the provider and organization is and what is to be provided.

Watts, S., & Raza, M. (2019, June 15). *SaaS vs PaaS vs IaaS: What's The Difference & How to choose*. BMC Blogs. https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/. Accessed September 21, 2023

Stephen Watts is a marketing professional and professional website developer, so he has experience with finding and working with service providers and the systems they use. Muhammad Raza is a computer scientist who works with the KTH Royal Institute of Technology and works in developing Cloud Computing and Security. They focus on the different kinds of infrastructure and varieties of Cloud Storage. They talk about SaaS, IaaS, and PaaS, but for this paper PaaS was not discussed. They describe the benefits of both SaaS and IaaS and in which situations and for what organizations they are best suited for, particularly based on size and growth. Then they describe the delivery of the services and how secure and reliable they are.