Rayyan Al Anani

Dr. Anthony Townsend

MIS 599: Creative Component

07/16/2021

Cloud Technology and Security

Contents

Abstract

Cloud security is a critical component in any firm's data management framework. As such it deserves serious attention. The rapid adoption of public cloud services necessitates businesses to find new ways of detecting and mitigating cloud security breaches.

This study investigates Cloud Storage Technology and the risks associated with it.
It explores the differences between Cloud storage systems and Traditional storage systems, the pros and cons of using Cloud over Traditional, security concerns, and risk mitigation of the threats associated with Cloud.
Individuals and organizations (end-users) often find it challenging to decide to adopt Cloud technology to store their information or whether to play it safe and go for the traditional way!

This study aims to provide a clearer view of the differences between Cloud storage and Traditional storage – with the hopes of helping the end user to determine the best approach needed for their needs!

1.0 Introduction

Cloud security is a critical component in any firm's data management framework that deserves serious attention. The rapid adoption of public cloud services necessitates businesses to find new ways of detecting and mitigating cloud security breaches. As firms share more data and applications to cloud-based platforms, the need to establish new practices to secure user data and safeguard it from unauthorized access, abuse, or corruption from third parties arises. To grasp the importance of Cloud Security, and what accompanies this technology from advantages, disadvantages and challenges, a detailed literature review was conducted. Moreover, this review addresses the issues associated with the maintenance and implementation challenges, on the security experts' part. The Increased sophistication in cloud computing threats compels organizations and firms to spend more on training personnel to be able to deal with the emerging threats.

In addition, this review also outlines problems with creating, storing and sharing passwords among end-users. It also compares traditional storage to cloud storage in regard to safety of data, ease of access, data management features, scalability and capacity (volume of data supported). Organizations that implement cloud storage must also understand the security challenges associated with storing their data off-site across multiple interconnected servers. organizations stand to gain immensely from understanding the benefits of implementing cloud storage and proven security measures.

2.0 Benefits of Using Cloud vs. Traditional Storage

Cloud storage is the new frontier in high-performance data storage. It has transformed the way organizations use, store and share data. In a study published in 2017, Radwan, Azer, and Abdelbaki noted that a growing number of organizations are shifting to cloud computing solutions in order to exploit the benefits of Big Data (Radwan et al., 2017) Currently, many firms around the world virtually collect and make use of large amounts of information relating to their customers. In doing so, cloud storage provides organizations with the opportunity to safely and conveniently store their data on remote servers where it can be managed and accessed remotely (Hussein & Khalid, 2016). One of the advantages of cloud storage is that service is delivered on demand with just-in-time capacity. For instance, the use of cloud computing facilitates just-in-time (JIT) manufacturing; a concept that minimizes flow time and waste in production wherein materials are made available at the right place at the right time (Shiralkar, 2017). Cloud computing enables this approach through universal access to shared data and resources in real time. In their article, Ibrahim, Hamlyn-Harris, and Grundy noted that cloud storage eliminates the need to create and manage a physical storage infrastructure as is the case with traditional systems (Amani et al., 2010). This benefit implies that firms will reduce operational costs significantly in terms of space, manpower and maintenance of physical storage devices. Cloud infrastructure includes software, hardware, routers, and networking tools that the service provider provides. Hussein and Khalid mentioned that end-users pay for cloud storage and related services according to their individual requirements such as increased storage capacity or improved data management capabilities, including remote access (Hussein & Khalid, 2016). Typically, the needs of one user may be different from another user. The end-users enjoy broad network access to data remotely within an on-demand environment across heterogeneous platforms (Al-Shqeerat et al., 2017). Generally, cloud storage technology is an innovation that represents the next frontier in information management and security.

Cloud storage is easy to manage as it provides users with a self-service model wherein users including organizations have the freedom to access specific resources and features without constantly contacting the service provider. Due to the fact that hardware and software maintenance responsibility lies on the cloud service provider, cloud storage is easier for organization to manage (Al-Shqeerat et al., 2017).

It is far easier to set up a cloud storage platform than to create a similar one on the premise as is the case with traditional systems. This is attributed to the high level of rapid elasticity, cost effectiveness and resource pooling mechanisms that are made available to users of cloud computing services (Al-Shqeerat et al., 2017). Therefore, implementing and maintaining cloud storage is relatively easier than traditional models where each device and storage application is purchased and configured separately.

The cost of managing large volumes of data has become one of the main concerns as companies seek to be more efficient in the marketplace. Obrutsky observed in his study that managing cost had become an integral aspect of competitiveness in today's markets (4). The initial cost of implementing cloud service has been a source of concern for many small and medium businesses (Liu and Yu 138; Abdalla and Varol 4). However, the evaluation of cloud services should not focus on the initial costs but on the return on investment that the service brings. In his study, Obrutsky also noted that being on a cloud service provides a company with easy access to data and saves time and money in the long run (4). Research by Liu and Yu reported that the cloud makes it easier to run projects because it eases access to information (138) Organizations are charged for only the space they use, reducing costs due to the pay-as-you-go system implemented by cloud providers (Lal and Bharadwaj 570). The pay-as-you-go system ensures that cloud base applications are cost-effective by allowing end-users to pay only for the features that they use.

Obrutsky found that eliminating the jobs necessary to keep a traditional storage system running can significantly reduce costs associated with data storage and security (4). This enables organizations to focus their resources on their main goal. Lal and Bharadwaj mentioned that cloud storage saves companies the costs associated with expensive IT upgrades (Lal and Bharadwaj 574).

Cloud services also provide extra bandwidth on demand eliminating the need to acquire extra physical space that requires effort, time and money and making it easier for organizations to focus on their core function.

Another advantage of modern cloud storage is that off-site data storage protects information during disasters. Today's organizations have a variety of risks, including natural disasters and fires that can lead to the loss of data stored on-site (Lal and Bharadwaj 570). Cloud systems have become a critical aspect of business continuity and disaster preparedness (Obrutsky 3). Businesses can easily recover data that is essential for everyday operations in the unfortunate case of unexpected data loss due to natural disasters.

3.0 Cons of Using Cloud Storage vs. Traditional Storage

Like any other technology or service out there, Cloud Services are also accompanied by some disadvantages. One of the main disadvantages of cloud storage is it relies on an internet connection. Obrutsky stated that network interruptions could interfere with access to data which can impact business operations (2). Traditional storage does not require an internet connection since the information is stored physically on the premises (Obrutsky 3). In cloud storage, user experience is limited by internet connection failure (Abdalla and Varol 6).

According to Abdalla and Varol, privacy is another main issue because cloud storage involves many organizations sharing one service provider, which increases the risk of access by external providers (4).

Like most services out there, you get what you pay for! According to Abdalla, customers have a hard time using the service when there is no adequate support from cloud service providers (Abdalla 4). Even though, there are some free cloud services out there, opting for a free cloud service will result in a poor support, which can impact access to the data.

Cloud storage also requires trust in the service provider. The reality is that many organizations should be prepared to lose control over their data when data is stored remotely. Traditional storage is more suited for organizations that need significant control over their data. Innovative companies that have valuable proprietary technology may find traditional storage to be more suitable.

On-site data storage provides organizations with direct management of security. Liu and Yu found that it is not uncommon for cloud providers to offer a level of privacy that does not support an organization's compliance with regulations (138). Signing to a cloud service requires compliance with the terms and conditions of the provider, leading to a loss of control.

There are instances when crowd traditional storage is better than cloud storage. In the complex threat environment, companies need to ensure their data is stored in a system with enhanced security and easy access (Mushtaq et al. 188). The same study by Mushtaq et al. noted that there are a growing number of threats surrounding cloud technologies (190). The risk increases when organizations do not have control over the security of their data.

4.0 Cloud Security Threats and Challenges

Cloud services face many security threats that can negatively impact end-users. There are diverse security threats that exist in networks and intranets. Research by Bonguet, and Bellaiche Denial-of-service (DOS) attacks have become an increasing threat when many users rely on the same cloud storage service (43). A DOS attack is meant to shut down a machine or network, denying end-users access to their data. This is done by overwhelming the targeted server with traffic that triggers a crash. DOS attacks are different than other types of cyber-attacks, due to the fact that attackers are not after stealing end-user's information. DOS attack's primary goal is to slow or take down a website. The incentive behind the attacks are diverse, ranging from simple fun, to financial gain and ideology. Bonguet and Bellaiche argued that security problems arise because cloud technology is a networked-based infrastructure that exposes users to external and internal attackers (43).

Cloud service providers have been dealing with sophisticated DOS attacks that flood their systems with huge volumes of unreal data that make the services unavailable when they are needed(Venkatesh and Eastaff. 1744).

Bonguet and Bellaiche warn that DOS attackers identify vulnerabilities and attack them simultaneously (43). When GoGrid was attacked in 2009, thousands of end-users could not access their data (Bonguet and Bellaiche 43).DOS attacks have become a leading threat to the security cloud computing models (Bonguet and Bellaiche 43). As cloud services become more popular, cybercriminals have developed sophisticated DOS attacks designed to extort users (Bonguet and Bellaiche 43). Since a cloud system can host many users, DOS attacks are common. For instance, research shows that there was a 15% increase in DOS attacks in the

first six months of 2020, where 4.83 million DOS were reported (Help Net Security). During this period, attackers mainly focused on the complex and emerging COVID-19 pandemic lifelines encompassing e-commerce, healthcare, and educational services. With the current pace of globalization, security has become a major issue of concern for companies that depend exclusively on cloud storage to operate and provide their services.

One of the main challenges facing the end users of cloud services is the unavailability of data on demand which occurs due to a DOS. From an end-user perspective, the inability to access data can severely impact operations (Mushtaq et al. 188). Organizations are wary of the potential unavailability of data because it impacts decision-making and business continuity (Venkatesh and Eastaff. 1744). DOS attacks can disrupt business operations for an extended period of time, causing massive delays and huge costs.

Cloud storage users also have to deal with the problem of data breaches. According to a study by Subramanian and Jeyaraj, data breaches on cloud storage service providers have increased in the last three years, indicating that data breaches is a growing issue (4). Amazon, Microsoft, and Dropbox cloud services have been breached and private customer data stolen by hackers (Subramanian and Jeyaraj 4). Venkatesh and Eastaff mentioned that end users began to realize that security is the leading challenge in cloud storage (1742). Data breaches negatively impact the reputation of an organization, since trust between the end user and the service provider is an integral part of cloud services usage. Unlike DOS attacks, Cloud data breaches are driven by theft of intellectual property (Hussein & Khalid, 2016). Radwan et al. pointed out that misconfiguration of cloud infrastructure can increase vulnerabilities to hackers (Radwan et al., 2017).

Compromised credentials are a constant security threat to cloud services. Credentials such usernames and passwords are usually handled by end-users who are required by their organization to adopt best practices to protect their information.

Venkatesh and Eastaff described data confidentiality as ensuring that only authorized customers can view the data (1742). Mushtaq et al. mentioned that it is not possible for cloud storage to achieve physical isolation because the data is transmitted through public networks (190).

Data confidentiality is not guaranteed in cloud computing compared to traditional in-house storage systems. Venkatesh and Eastaff examined cloud security challenges and found that cloud service providers usually require that their customers change identity and access management practices for improved data security (1743). For instance, Google is currently on a mission to prevent its users from reusing their passwords and require them to change the passwords, at least once every 60 days (Allison; Peters). Research further shows that " in 2019, about "44 million Microsoft accounts used logins that had been leaked online" due to poor password and other user access and management practices (Peters). Inadequately protected credentials are a significant threat to the security of cloud storage (Mushtaq 184). Apart from service providers, users have a responsibility to maintain high-security standards. Failure to implement autorotation cryptographic keys, certificates, and passwords can lead to unauthorized access of data (Mushtaq et al. 191). Failure to use multi-factor authentication also contributes to cloud data breaches (Mushtaq 188). The main challenge with passwords is that people write them or give them to colleagues (Weber and Rudman8). Hackers have also turned to impersonation in order to access data.

Integrity is another serious problem in cloud computing. This aspect concerns the manner in which data is stored and accessed over the cloud to prevent unauthorized access, deletion and

any kind of modification. Since cloud storage is a sharing resource, the risk of the integrity of the data being breached is high (Venkatesh, and Eastaff 1744). However, according to a study by Venkatesh and Eastaff, when data is safeguarded by authorized persons and is therefore considered to be accurate and protected from unauthorized users and deletion (1744).

Obrutsky stated that traditional storage systems are relatively safer because they are in-house and more difficult to modify (3). Therefore, it is important for the user to closely monitor the data to ensure that it is not corrupted (Mushtaq et al. 192). Data integrity tools may fail to identify corrupted data causing irreparable damage to the organization (Mushtaq et al. 190). Users usually demand proof that their data will not be modified while in the cloud (Venkatesh, and Eastaff 1744). Cloud services invest in encryption technologies in order to safeguard the data from being corrupted.

Trust is an important factor in cloud storage security. It takes time and is challenging to assure people and businesses that data or people will behave in a certain way (McLeod and Gormly 350). For organizations to comfortably use a service, they need to fully trust that their data is protected and secure from unauthorized third-party access. According to McLeod and Gormly, even users on the cloud still do not trust cloud storage because of security-related issues (McLeod and Gormly 350). Trust in cloud storage is impacted by the various security issues that increases the risk of data breaches or data unavailability (McLeod and Gormly 350). Trusted cloud service providers provide security and ensure the confidentiality and integrity of the data (McLeod and Gormly 350). According to Mushtaq et al., Users have the expectancy that cloud service is trustworthy in terms of security and availability (Mushtaq et al. 199). Because of the trust issues mentioned previously, many organizations still prefer the traditional storage system because it provides them with control of their data (Obrutsky 3).

Another challenge associated with Cloud services, is the lack of visibility that providers have over the end-user's activity. Radwan cautioned that security professionals lack the visibility they need to respond to most of the treats (Radwan et al., 2017). It is difficult to prevent malicious activity in this era where employees download mobile applications to solve work-related problems (Venkatesh and Eastaff 1744). Some of the applications downloaded by the employees on the devices connected to the cloud, do not meet the security requirements provided by the cloud service provider. It is difficult for security professionals to identify risks that are posed by an unsanctioned application (Mushtaq et al. 191). Unauthorized personnel can use such applications to access data stored on cloud storage (Mushtaq et al. 191). On-site protections and defenses posed by the company (end-user) become irrelevant when the organization lacks control over home network security and the practices of its employees.

Best practices in authentication access management are necessary to reduce the risk of security breaches. Venkatesh and Eastaff argued that every device is assigned a unique password (1742). Each employee is required to change their passwords regularly (Liu and Yu 140). Since it is difficult to keep on memorizing new passwords, employees tend to write the passwords down, which increases the risk of unauthorized access to data (Mushtaq et al. 188). Password managers can also provide other people with access to passwords. Cloud security is only effective if employees of organizations comply with regulations.

Even though, remote access is one of the advantages of cloud services, it is also considered to be one of the main reasons behind security breaches. Remote access allows hackers to exploit vulnerabilities on the network. Islam, Manivannan, and Zeadally believed that Users might not be aware that their interface is not secure (272). Islam et al. also found that hackers can exploit remote access by exploiting authentication through APIs (272). The larger the API infrastructure, the greater the risk of unauthorized data access (Islam 272). Due to the increased

importance of being vigilant when accessing data remotely, organization have now paid greater attention to how their employees access data remotely, as failing to do so can pose a serious security threat.

Security solutions that rely on implementing traditional security approaches such as a perimeter security model to protect the cloud infrastructure are ineffective. Perimeter security is comprised of systems like firewalls and browser isolation systems which are very preliminary in our current day and age. According to Ibrahim, Hamlyn-Harris, and Grundy, they have limitations because they are required to trap every system call before forwarding it to the hypervisor (Amani et al., 2010). Ibrahim et al. also noted that traditional security approaches cannot prevent attacks between the virtual machines and the V switch. A virtual switch (vSwitch) is a software application that allows communication between virtual machines.

The main challenge is that conventional security approaches continue to be used despite the cloud complexity that results from the dynamic changes that take place in the cloud (Amani et al., 2010). The failure to implement security solutions that are designed for the complexities of the cloud storage infrastructure is a major security concern in today's world. Failure to do so, can lead to various security breaches and major data loss.

The reality is that the virtual architecture of the cloud are pushing the physical boundaries that are traditionally used to define, manage and protect organizations (Amani et al., 2010). Cloud technologies have a major hurdle when it comes to developing solutions that effectively protect the virtual cloud infrastructure

Despite the numerous benefits of implementing cloud service mechanisms across different functionalities of an organization, the major drawback of this digital phenomenon is an increase in security threats. Among the most notable threats to cloud computing resources is account hijacking. Today, it is possible for a hacker or a group of hackers to penetrate a cloud storage

service upon gaining credential information about a targeted user through such methods as surveillance of online activities or examining cookies (Idris et al. 19). Whichever way hackers manage to hijack a cloud user's account, this vulnerability continues to be considered a serious threat to cloud computing and may restrict its uptake in some organizations. Tirumala et al. (1) describe account hijacking as a type of identity theft that aims to deceive end-users. A good example is The New York Times website hack by the Syrian Electronic Army (SEA) that led to a downtime of about 6 hours. Typically, attackers in these kinds of threats often gain access to a user's cloud account through impersonation using phishing and spoofing emails or even pop-up messages.

Security experts over the world recommend mitigating such risks by formulating and deploying an appropriate incident response plan. Here, the Be ready to Face (BRF) strategy has proven to be effective wherein one expects the worst possible security scenario and learning from past mistakes (Tirumala et al. 5). Besides account hijacking, cloud computing is susceptible to service hijacking. In this kind of threat, attackers gain unauthorized access or control over specific cloud applications using phishing, fraud or by deploying custom-made software into a service (Idris et al. 20). Thus, cloud service account administrators should be vigilant for account and service hijacking threats.

Cloud computing is also faced with the threat of data loss and leakage. At times, data is lost within a cloud platform due to the vast amount of information held in the infrastructure. It is not uncommon to find that some packets of information are lost during transmission due to corruption or failure in the physical network configuration (Ariffin et al. 401). Hackers may exploit some of these failures and take advantage of a compromised cloud framework. Cloud technologies such as hypervisor can express the vulnerability of possible loss of data and data leakage. A hypervisor, also known as a virtual machine monitor or VMM, is software that

creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing ("Hypervisor", 2021).

A good example that demonstrates the impact that data leakage can cause is Exactis, an advertising company, data leakage that exposed information of 340 million clients (Ariffin et al. 400). Moreover, DOS attacks can also cause data loss (Idris et al. 20). Nowadays, such attacks are prevented by reinforcing firewalls with in-build algorithms based on machine learning techniques to detect cyber-attacks.

5.0 Mitigation of Risks by Cloud Service Providers

Cloud service providers such as Amazon and Google implement different strategies to ensure risk mitigation. Among the most familiar security risks associated with cloud storage services is Denial of Service (DoS) attack. These are well-known threats that have the potential of causing high impact damages on internet and/or network services. Typically, black hat hackers implement such malicious attacks through deployment of botnets that lead to flood attacks wherein oversaturation of resource limits or denies users access to certain resources (Ubaid-Ur-Rahman and Srinivasan 3633). Essentially, this security threat targets the availability of web-based applications. The main approach to mitigate risks related to DoS includes among other strategies: firewall configuration that detects malicious activities and implements security policies that only grants access to trusted sources when reviewing web server requests (Ubaid-Ur-Rahman and Srinivasan 3637). Here, algorithms can be formulated to prevent specific botnets from manipulating access privileges in a cloud service network. A DoS protection mode can be adopted, in which traffic from genuine sources are allowed whereas traffic from other sources are placed on protection mode pending review for possible flood attacks. For instance, Microsoft provides customers of its Office 365 products with multilayer security that protects them from DoS attacks by masking how data is being transferred during usage (Bhardwaj and Goundar). Therefore, it is advisable to protect cloud-based services from Denial-of-Service attacks by configuring network infrastructure with robust security mechanisms.

Besides DoS attacks, cloud-based storage is susceptible to a wide variety of data breaches. One notable form of data breach worth highlighting is malicious insider, which is an attack that originates from inside an organization. In 2011, a survey of 607 businesses established that approximately 21% of cyber threats are initiated by insiders (Chou 83). The malicious insider

threat may entail any of the following: unauthorized access and improper use of corporate data, virus infection, exposure of confidential information, theft of intellectual property and installation of malicious code (Chou 83).

Online cyber theft is another form of data breach. Cyber thieves may steal digital media and personal information such as email and phone numbers of users on social media networks or cloud-based services such as Amazon's EC2 service. A possible defense strategy that addresses data breaches is multi- factor authentication. The Cloud Security Alliance (CSA) not only compels organizations such as Google, Amazon and Facebook to caution users from sharing credentials among themselves, it also advocates for the use of multi-factor authentication which combines information of what someone knows or possesses with something that they are (Mosca et al. 534). This combination of security credentials makes it difficult for potential hackers to infiltrate a cloud user's account to steal, manipulate or share sensitive data.

Another security threat that characterizes cloud services today is related to the confidentiality of data. Haider and Selvan (1) point out that in cloud services, the information of customers is stored in remote services and managed by third parties with access to the same facilities over the internet. Most people are afraid of storing corporate data on the cloud for fear of exposure to unauthorized persons. Currently, this fear of data getting to the wrong hands significantly limits the growth potential of cloud technology. Thankfully, there are numerous mitigation techniques that organizations such as Amazon and Microsoft have embraced to guarantee customers of the confidentiality of their data. Biometric encryption (BE) is a familiar method of securing data that entails biometric encryption of user data wherein the authorized user is identified through biometrics such as facial properties and fingerprints (Haider and Selvan 1). In regards to access, the security method applies a BE binding algorithm that generates a security key that is biometrically encrypted. Haider and Selvan (3) state that in this framework,

sensitive user data is secured in a private cloud prior to being uploaded to a public cloud infrastructure. The other technique that Google and other cloud service providers apply a combination of encryption with obfuscation whereby encryption uses algorithms whereas obfuscation uses mathematical functions and robust programming techniques. It is proven that encryption and obfuscation on the user's end substantially improves the security of sensitive data.

Furthermore, one of the mitigation strategies to prevent data loss and leakage is through the deployment of special agents. For instance, In its effort to prevent data leakage and loss over the cloud, Google Inc. suggests the use of " specialized agents to produce telemetry about user and host activity in cloud-based virtual machines (VMs)"("Google Cloude"). Doing so provides the Security Operations Center (SOC) with a clear visibility of the abnormal activities that may compromise information security. Data loss and data leakage are common security threats that cyber security experts are faced with in the context of cloud environments. The loss or leakage of crucial data may have severe impacts on the productivity and profitability of any given organization. In addition, providers that experience these challenges tend to lose the trust of its' users.

Studies show that data leakage is among the critical security challenges. 88% of respondents in a survey feel that data leak prevention is the most important (Rao and Selvamani 206). Thus, it is essential to protect data from these kinds of threats for long-term sustainability. A powerful mitigation approach to loss and leakage of data is data back-up on secondary drives (Rao and Selvamani 208). This method of securing data from possible loss or leakage is currently adopted by leading cloud-based services such as Amazon.

Cloud service providers typically adopt a model that clearly defines shared responsibilities. Some familiar service models that providers offer include Infrastructure as a Service (IaaS)

model and the Software as a Service (SaaS) model. The model chosen by the customer is well-defined and outlines the shared responsibility as expressed in an agreement between the provider and the client (Maniah et al. 268). This measure is crucial in the elimination of risks that are associated with cloud-hosted services. In addition, it is important for corporate clients to understand the nature of the shared responsibility models that is provided by cloud service provider (Ramachandra et al. 223).

6.0 Why Some Companies Choose Traditional Storage Over Cloud Setups.

Even though the countless benefits of cloud computing are sufficiently convincing, some organizations choose to rely on traditional modes of storage for their data resources. One of the reasons for making this decision is that cloud storage is dependent on the availability of the internet, hence for continued access to cloud services a firm requires a stable internet connection with decent bandwidth (Mukherji and Srivastava 850). Low bandwidth restricts the full utilization of cloud functionalities as users will seek to upload text and multimedia information on a regular basis. In some cases, reliable internet connections deliver poor performance owing to high latency. Mukherji and Srivastava (850) found that if multiple users continuously access cloud features concurrently the quality-of-service access tends to deteriorate. There is also the issue of price wherein the cost of acquiring a cloud service plan is relatively higher than traditional storage options. Chen et al. (104) note that cloud computing is associated with high capital expenditure that companies have to take into account before committing. Apart from the initial cost, organizations may deter from implementing cloud-based storage because of the security risks associated with cloud technology. The major challenge in securing cloud computing services is the provider ensuring that each user's data remains private from other users (Sen and Tiwari 69). Therefore, it becomes crucial for cloud storage providers to adopt robust security measures that secure data while ensuring availability of applications to multiple users.

7.0 The Current Uptake of Cloud Services by Enterprises.

In the current business industry, more firms are moving their storage operations towards the cloud in massive proportions. This trend is attributed to the numerous benefits of cloud-based technologies compared to traditional methods of storage, including remote access to data at any time, on-demand services, reliable data storage and access, off-site backup, effective use of bandwidth, cost-effectiveness and data protection (Liu and Yu). Today, the use of cloud-based solutions is substantial across nations and industries. A survey by Statista; a German company specializing in market and consumer data, revealed that the proportion of corporate data held in cloud infrastructure in the world increased from 30% in 2015 to 50% as of 2020 (Mlitz). Most of this data is in the form of backup in case an organization loses its existing traditional data resources. Many firms in Europe are constantly shifting their storage functions to cloud environments with the aim of achieving higher levels of reliability and security. As of 2021, approximately 36% of companies within the European Union block; the largest trade block in the world, have implemented cloud computing for file management and e-mail services (Eurostat). Here, firms use two main services of cloud computing: software applications and cloud infrastructure. Cloud storage is playing a vital role in the reduction of downtime and data loss for organizations of different sizes. A five-year survey by Unitrends revealed that 30% of organizations enrolled in the study reported losing data as a result of outages in their data centers (Unitrends). Cloud computing provides such enterprises with effective tools to manage the problem, including Disaster-Recovery-as-a-Service (DRaaS), reliable backup and recovery applications.

8.0 The Cost of Traditional Storage Systems Versus Cloud Service.

In terms of cost, cloud storage delivers better value than traditional or in-house storage. Internal storage is associated with high operating costs and high physical capacity, while these services are offered at low cost in the cloud (Reichman 3). Traditional storage infrastructure is expensive to purchase, install and maintain. Forrester Research Inc. estimates the cost of storing and managing 100TB of data in the internal model to be $955,500 (Reichman 8). This cost includes base storage acquisition, data copies, warranty, power charge and other factors. On the other hand, a cloud service such as Amazon provides a small storage price per GB of about $0.118 whereas the one would spend $4 per usable GB under internal storage model (Reichman 8). For cloud storage, base rate determines the overall cost of running the platform for various organizational settings. Here, it is important to understand that prices vary from one vendor to the next.

Traditional storage cost has various determinants that ought to be considered when conducting a full cost accounting. According to Information Lifecycle Management models the key factors that define the cost of traditional storage include: energy or utility cost, rental cost, initial purchase of storage equipment, service, environmental cost and the cost of disposal (Dutta and Hasan 4). Energy cost is divided into different components such as network and servers, cooling, security, infrastructure among other resources. Service costs are generally composed of purchase of software, repair of hardware components, network management, cooling maintenance and power services (Dutta and Hasan 4). Here, organizations incur the cost of the price of disks, floor accessories, cooling fans, networking components such as switches, routers and cables. Floor rent is a major determinant of traditional storage costs. For example, a data center in Manhattan costs about $0.1 per square feet each month (Dutta and

Hasan 4). Some organizations may opt to build their own data centers, and this is usually expensive.

Disposal of physical storage devices requires specialized machines that are expensive. In regard to the environment, firms often purchase backup generators that complement main power supplies. These are sources of harmful gases that destroy the ozone layer and contribute to global warming (Dutta and Hasan 4). The initial cost of a CIS data center with 4 server racks with each rack holding 9 units is approximately $114,000 (Dutta and Hasan 8). Therefore, cloud storage is preferred to traditional storage on the basis of annual cost of operation.

9.0 Recommendation and Conclusion

Cloud storage requires trust in the service provider. The reality is that organizations should be prepared to lose control over their data. Traditional storage is more suited for organizations that need significant control over their data, which is the main issue of concern for cloud computing and storage. Innovative companies that have valuable proprietary technology may find traditional storage to be more suitable. On-site data storage provides organizations with direct management of security. It is common for cloud providers to offer a level of privacy that does not support an organization's compliance with regulations yet signing to a cloud service requires compliance with the terms and conditions of the provider, leading to a loss of control.

As cloud computing continues to gain widespread popularity in many organizational applications, the main shortcoming of this global trend is the existence of various types of security threats and challenges. Some of the common security threats that are associated with cloud technology infrastructure are account and service hijacking, denial of service attacks and data leakage and loss. Additionally, deploying and running cloud storage in an organization carries a series of challenges that requires expert attention. Here, issues such as violation of data confidentiality, concerns about integrity of data during transmission, availability, data segregation, authentication and authorization are major limitations to a successful cloud service operation. For instance, hacked cloud platforms result in long downtimes that injure a brand's reputation and profitability. Nowadays, some firms choose to go for cloud storage over traditional methods to exploit the numerous benefits of cloud computing. Currently, many enterprises have embraced the benefits of cloud storage as many companies have shifted to cloud-based services such as backup and remote access. Indeed, cloud offers better reliability and effectiveness than traditional models as it addresses downtime and loss of data. The cost benefit comparison between cloud and traditional storage favors cloud computing. In-house

storage has relatively high operational costs whereas cloud services provide a wide range of data management features at affordable prices. However, implementing cloud storage requires organizations to tailor their own data processes to use cloud storage. Despite this limitation, cloud storage provides organizations with better price on storage space and annual cost savings.

Overall, cloud storage provides a wide set of advantages and functionalities in comparison to the traditional approach to data storage. In particular, cloud storage is more effective as it uses a virtual hosting solution and there is no need to have the physical hardware and servers that are common with the traditional storage approach. For this reason, the customer and the client will not need to invest a lot of resources to acquire the physical servers since the storage space can readily be rented by cloud service providers at incredibly low prices, with additional layers of data security provided using modern data encryption techniques. In addition, the use of cloud services ensures that there is more resilience and elasticity

Works Cited

Abdalla, Peshraw Ahmed, and AsafVarol.“Advantages to Disadvantages of Cloud Computing for Small-Sized Business.”2019 7th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2019

AbubakarIdris, Usman, et al. "Security Threat on Cloud Computing." *International Journal of Computer Trends and Technology*, vol. 37, no. 1, 2016, pp. 18-21, www.researchgate.net/profile/Jamilu-Awwalu/publication/308302020_Security_threat_on_Cloud_Computing/links/595a4bce0f7e9b897eab3558/Security-threat-on-Cloud-Computing.pdf?origin=publication_detail.

Allison, Peter, R. (2016). The problem of passwords and how to deal with it.www.computerweekly.com/feature/The-problem-of-passwords-and-how-to-deal-with-it

Al-Shqeerat, Al-Shrouf, Mustafa, and Hassan, Rehanie. “Cloud Computing Security Challenges in Higher Educational Institutions-A survey.” *International Journal of Computer Applications*vol.161, no. 6 2017 pp. 22-29.

An, Y Z et al. "Reviews On Security Issues And Challenges In Cloud Computing". *IOP Conference Series: Materials Science And Engineering*, vol 160, 2016, p. 012106. *IOP Publishing*, doi:10.1088/1757-899x/160/1/012106. Accessed 10 July 2021.

Bonguet, Adrien, and Martine Bellaiche. “A Survey of Denial-Of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing.” *Future Internet* vol. 9, no. 3 2017 p. 43.

Bhardwaj, Akashdeep, and Sam Goundar. “Cloud Computing Security Services to Mitigate DDoS Attacks.” *Cloud Computing Security - Concepts and Practice*, 22 July 2020,

www.intechopen.com/books/cloud-computing-security-concepts-and-practice/cloud-computing-security-services-to-mitigate-ddos-attacks.

Chou, Te-Shun. "Security Threats on Cloud Computing Vulnerabilities." *International Journal of Computer Science and Information Technology*, vol. 5, no. 3, 30 June 2013, pp. 79–88, www.researchgate.net/publication/289756317_Security_Threats_on_Cloud_Computing_Vulnerabilities/fulltext/57a5d1d108aefe6167b61ea0/Security-Threats-on-Cloud-Computing-Vulnerabilities.pdf?origin=publication_detail, . Accessed 27 Apr. 2019.

Haider, Yusuf, and Siva Selvan. *Confidentiality Issues in Cloud Computing and Countermeasures: A Survey*. July 2016, pp. 1–5, www.researchgate.net/profile/Sivaselvan-N/publication/305689086_Confidentiality_Issues_in_Cloud_Computing_and_Countermeasures_A_Survey/links/5799f1af08aeb58230786535/Confidentiality-Issues-in-Cloud-Computing-and-Countermeasures-A-Survey.pdf?origin=publication_detail.

Hypervisor. (2021). Retrieved 22 July 2021, from https://www.vmware.com/topics/glossary/content/hypervisor

Mosca, Patrick, et al. "Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services." *International Journal of Communications, Network and System Sciences*, vol. 07, no. 12, 2014, pp. 529–535, www.researchgate.net/publication/276499055_Cloud_Security_Services_Risks_and_a_Case_Study_on_Amazon_Cloud_Services/fulltext/5abff05345851584fa73fbf6/Cloud-Security-Services-Risks-and-a-Case-Study-on-Amazon-Cloud-Services.pdf?origin=publication_detail, . Accessed 2 June 2019.

Chen, Thomas, et al. "The Perceived Business Benefit of Cloud Computing: An Exploratory Study." *Journal of International Technology and Information Management*, vol. 25, no. 4, 2016, pp. 100-122, scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1297&context=jitim&httpsredir=1&referer=.

Dutta, Amit, and RagibHasan. *How Much Does Storage Really Cost? – Towards a Full Cost Accounting Model for Data Storage*. Alabama. www.researchgate.net/profile/Ragib-Hasan-4/publication/295399942_How_Much_Does_Storage_Really_Cost_Towards_a_Full_Cost_Accounting_Model_for_Data_Storage/links/572d032708aee022975982cb/How-Much-Does-Storage-Really-Cost-Towards-a-Full-Cost-Accounting-Model-for-Data-Storage.pdf?origin=publication_detail.

Endo, Patricia T., et al. "High availability in clouds: systematic review and research challenges." *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 5, no. 16, 2016, pp. 1-15, journalofcloudcomputing.springeropen.com/track/pdf/10.1186/s13677-016-0066-8.pdf.

Google Cloud. https://cloud.google.com/security/data-loss-prevention/preventing-data-exfiltration

Help Net Security www.helpnetsecurity.com/2020/09/30/4-83-million-ddos-attacks-first-half-of-2020/

Hussein, Nidal Hassan, and Ahmed Khalid.“A survey of cloud computing security challenges and solutions.”International Journal of Computer Science and Information Security vol. 14no.1 2016 pp. 52.

Ibrahim, Amani S., James Hamlyn-Harris, and John Grundy. “Emerging security challenges of cloud virtual infrastructure.” arXiv preprint arXiv:1612.09059 (2016).

Islam, Tariqul, D. Manivannan, and SheraliZeadally. “A Classification and Characterization Of Security Threats In Cloud Computing.” *International Journal.Next-Generation.Computer*vol.7 no. 1 2016 pp. 268-285.

Jathanna, Rohan, and DhanammaJagli."Cloud Computing and Security Issues." *International Journal of Engineering Research and Application*, vol. 7, no. 6, 2017, pp. 31-38, www.researchgate.net/profile/Dhanamma-Jagli/publication/317908867_Cloud_Computing_and_Security_Issues/links/5a701b9ca6fdcc33daa804fa/Cloud-Computing-and-Security-Issues.pdf?origin=publication_detail.

Lal, Prerna, and Sangeeta Shah Bharadwaj.“Understanding the impact of cloud-based services adoption on organizational flexibility.” Journal of Enterprise Information Management 2016 vol. 29 no. 4, pp. 566-588.

Liu, Allan, and Ting Yu. “Overview of Cloud Storage And Architecture.” International Journal of Scientific & Technology Research 2018pp. 136-149.

Maniah et al. "Survey On Threats And Risks In The Cloud Computing Environment". *Procedia Computer Science*, vol 161, 2019, pp. 1325-1332. *Elsevier BV*, doi:10.1016/j.procs.2019.11.248.

McLeod, Julie, and Brianna Gormly.“Using the cloud for records storage: issues of trust.”Archival Science vol. 17 no. 1 2017 pp. 349-370.

MohdAriffin, Muhammad A., et al. "Data Leakage Detection in Cloud Computing Platform." *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1.3, 2019, pp. 400-408, www.researchgate.net/profile/Muhammad-Azizi-Mohd-

Ariffin/publication/335190617_Data_Leakage_Detection_in_Cloud_Computing_Platform/links/5d7622a74585151ee4a9058d/Data-Leakage-Detection-in-Cloud-Computing-Platform.pdf?origin=publication_detail.

Mukherji, Sandeep, and ShashwatSrivastava."Pros and Cons of Cloud Computing Technology." *International Journal of Science and Research (IJSR)*, vol. 5, no. 7, 2015, pp. 848-851, www.ijsr.net/archive/v5i7/ART2016314.pdf.

Mushtaq, Muhammad Faheem, UroojAkram, Irfan Khan, SundasNaqeeb Khan, AsimShahzad, and ArifUllah.“Cloud computing environment and security challenges: A review.”*International Journal of Advanced Computer Science and Applications* 8.10 (2017): 183-195.vol. 8 no. 10 2017 pp. 183-195.

Obrutsky, Santiago. “Cloud storage: Advantages, disadvantages and enterprise solutions for business.”*Proceedings of the Eastern Institute of Technology Conference*. 2016.

Paudel, Samana. "Data Breach a Cybersecurity Issue in the Cloud." Aug. 2019, pp. 1-6, www.researchgate.net/profile/Samana-Paudel/publication/335243297_Data_Breach_a_Cyber_Security_Issue_in_Cloud/links/5d5aefba458515210252202f/Data-Breach-a-Cyber-Security-Issue-in-Cloud.pdf?origin=publication_detail.

Peters, Jay. Google is on a mission to stop you from reusing passwords. Jun 23, 2020www.theverge.com/2020/6/23/21299007/google-password-checkup-security

Radwan, Tarek, Marianne A. Azer, and NashwaAbdelbaki.“Cloud computing security: challenges and future trends.”*International Journal of Computer Applications in Technology* vol. 55 no. 2 2017 pp. 158-172.

Ramachandra, Gururaj et al. "A Comprehensive Survey On Security In Cloud Computing". *Procedia Computer Science*, vol 110, 2017, pp. 465-472. *Elsevier BV*, doi:10.1016/j.procs.2017.06.124. Accessed 10 July 2021.

Reichman. *File Storage Costs Less In The Cloud Than In-House*. Forrester, 2011. media.amazonwebservices.com/Forrester_File_Storage_Costs_Less_In_The_Cloud.pdf.

Rao, R. Velumadhava, and K. Selvamani. "Data Security Challenges and Its Solutions in Cloud Computing." *Procedia Computer Science*, vol. 48, 2015, pp. 204–209, www.researchgate.net/publication/277935944_Data_Security_Challenges_and_Its_Solutions_in_Cloud_Computing/fulltext/55e08d3308aede0b572e8d52/Data-Security-Challenges-and-Its-Solutions-in-Cloud-Computing.pdf?origin=publication_detail, .

Ubaid-Ur-Rahman, Mohd, and M Srinivasan. "A Critical Analysis of Denial of Service (Internet and Network Service) Attacks and Their Detection." *Journal of Critical Reviews*, vol. 7, no. 12, 2020, pp. 3632–3639, www.jcreview.com/fulltext/197-1599142183.pdf

Sen, Arun K., and Pradeep K. Tiwari. "Security Issues and Solutions in Cloud Computing." *IOSR Journal of Computer Engineering*, vol. 19, no. 2, 2017, pp. 67-72, www.researchgate.net/profile/Pradeep-Tiwari-3/publication/316922625_Security_Issues_and_Solutions_in_Cloud_Computing/links/5a9e16f20f7e9bc35fcfd124/Security-Issues-and-Solutions-in-Cloud-Computing.pdf?origin=publication_detail.

Shiralkar, Kedar. "Just-In-Time Manufacturing Using Cloud Computing." International Journal of Engineering and Techniques, vol. 3, no. 6, Nov. 2017, pp. 405–408, oaji.net/articles/2017/1992-1515751789.pdf.

Subramanian, Nalini, and Andrews Jeyaraj. "Recent Security Challenges In Cloud Computing 2018, vol.71, pp. 28-42.

Sun, Yunchuan et al. "Data Security And Privacy In Cloud Computing". *International Journal Of Distributed Sensor Networks*, vol 10, no. 7, 2014, p. 190903. *SAGE Publications*, doi:10.1155/2014/190903.Accessed 10 July 2021.

Tirumala, Sreenivas S., et al. "Analysis and Prevention of Account Hijacking Based Incidents in Cloud Environment." *2015 International Conference on Information Technology (ICIT)*, 2016, pp. 1-7, www.researchgate.net/profile/Sreenivas-Sremath-Tirumala/publication/284158931_Analysis_and_Prevention_of_Account_Hijacking_based_INCIDENTS_in_Cloud_Environment/links/56a743cf08aeded22e36c1bb/Analysis-and-Prevention-of-Account-Hijacking-based-INCIDENTS-in-Cloud-Environment.pdf?origin=publication_detail.

Venkatesh, A., and Marrynal S. Eastaff. "A study of data storage security issues in cloud computing." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* vol. 3 no. 1 2018 pp. 1741-1745.

Weber, Lyle, and Riaan J. Rudman. "Addressing The Incremental Risks Associated With Adopting Bring Your Own Device." *Journal of Economic and Financial Sciences* vol. 52 no. 11 2018 pp. 1-13.