The Safety of End-User Data in the Cloud

Rocky Goins

East Carolina University

Abstract

Data security is a serious issue in cloud computing because of the location of use data in different places across the world. This paper will discuss the security and privacy of end user data in cloud computing. The paper will delve into the details of data protection measures used to ensure maximum data protection while reducing the risks to user data. This research paper will also compare existing research on the techniques and approaches used to secure user data on cloud platforms.

Keywords: cloud computing, technology, innovation, internet, virtual, network, management, Google, IBM, Amazon, configuration, security.

Contents

Introduction

Cloud computing is projected to be a $200 billion industry by 2020. Businesses have reaped numerous benefits from cloud storage such as scalable storage for files and applications and saved time and financial resources by eliminating the need to build a capital-intensive data centers. Despite the myriad of benefits offered by cloud computing, most businesses have one major concern-the safety of end-user data in the cloud. Since the advent of cloud computing, there has been no greater priority for end-users than the safety and privacy of their data. With cloud service and storage solutions such as Microsoft Azure and Google cloud, it may come as a surprise that only ten per cent of the world's data is stored in the cloud which raises the question: what is holding users from storing data in the cloud. What this mainly boils down to whether an individual or a business can trust another party to store its data (Gonzales et al., 2017).

Risks of Storing Data

An article by Mathew Wall explores the risks of storing user data in off-premise cloud solutions. According to the author, the biggest risk lies in giving up control of user data to data centers operating in remote locations (Wall, 2016). Putting one's data next to another person's data also increases the risks of the data being lost, corrupted or stolen. There is also the tendency of assuming that the third-party cloud provider is fully responsible for maintaining the security of data. Wall also notes that data security largely depends on the quality of the cloud provider compared to that of an organization's IT department. Most data breaches that have occurred over the past three years have been from on premise systems rather than cloud solutions. However, there is always the inherent threat that personnel working for the cloud provider can introduce loopholes in the system.

Companies, businesses and institutions have increasingly migrated to cloud services such as Amazon Drive, Dropbox, Google Drive, and Microsoft OneDrive just to name a few. There is no doubt that these users are concerned about the safety of their data which partly explains why some users are still reluctant to use these services. Although data stored in the cloud is stored in an encrypted form, where the keys are held varies among cloud service providers. There are two main ways used to store data encryption keys. These keys can either be stored by the cloud service itself or by individual users. Most cloud services store the key, only allowing access to the key when the user logs in with their password. This not only convenient but also much safer than having individual users keep the keys. Nonetheless, it also less secure. If another person manages to access these keys, data may be stolen or corrupted without the knowledge of the legitimate user. According to Khan & Tuteja (2015), users can protect their data by combining features of the two approaches. Users should use their own encryption software to encrypt data before moving it to the cloud. When accessing the file, the user will be forced to download and decrypt the data.

The plethora of cloud service providers make it difficult for users to determine exactly how safe their cloud is. This is exacerbated by the lack of standardization in the industry. A cloud

service provider could top-of-the-line security features but lack of a unifying set of clear-cut guidelines makes it problematic for users to determine how safe a particular cloud solution is. News of a cyber-espionage (Dragonfly) hacking through cloud storage of petroleum energy operators, energy grid operators, and electricity generation plants are all over the cyber world. In addition to the legislation and policies put in place to protect user data in off-premise cloud platforms, the user plays a fundamental role in determining how and in what shape data is stored. Puthal et al. (2015), advises users of the cloud to avoid storing sensitive data in the cloud. Having a strong password can also help to protect data. No matter how high the level of security, a weak password introduces weak links in the security framework. The author underscores the importance of having IT experts and various security systems to back up data protection measures such as encryption and passwords.

Puthal et al. (2015) assert that the cloud is inherently safe but major breaches have reduced the public's confidence. In 2017, LinkedIn, Google Drive, and Evernote, all household names, suffered breaches. The world's largest US wireless carrier (Verizon) had accounts of over six million users exposed due to a misconfigured setting in the cloud as a result of human error. Most cloud services rely on a common infrastructure and open source code. This implies that a vulnerability can easily affect many service providers. A good example is the 2014 Heartbleed bug that can still affect providers due to a vulnerability in the OpenSSL protocol. Ali et al. (2015) opine that not all threats are malicious. Staff can introduce vulnerabilities in cloud storage due to human errors. It is vital that the staff is trained to understand the tools they use and how to handle user data. According to Muppidi et al. (2016), only one in ten cloud service providers in operation today follow industry best practices for protecting data.

One cannot overlook the power of government surveillance where cloud service providers have to surrender user data upon request. Companies such as Microsoft, Facebook, Google and Apple have in the past surrendered data to the U.S government because they are required to comply by law (Lustgarten, 2015). The risk of a cyber-attack arises anytime data is stored on the internet is of big concern. The risk is particularly heightened on the cloud, where volumes of data belonging to different users are stored on the same platform. The scariest threat is a Distributed Denial of Service(DDoS) attack. A successful DDoS attack can impact very many users because it is easier to steal or corrupt data in bulk (Somani et al., 2017). Although cloud providers have enacted stringent security measures, cyber-attacks have also become more sophisticated. When cloud providers get their security measures right, hackers come up with creative ways of accessing user data. For example, instead of breaching the cloud, hackers may try to breach accounts. Therefore, passwords and security questions become the weak link in an organization's security system.

Safely Storing Data

John Miller, PhD in distributed systems, strongly believes that files stored in cloud services are the most secure files. He attributes this to redundancy, security, and safe sharing. Cloud services stores at least three copies of data in different locations. Data can only be lost when the three copies of data disappear. Distributive storage complements encryption and authentication by storing data in multiple cloud databases. Therefore, maximum security is achieved by dividing the user's data into chunks and storing them in different databases. Encrypting and distributing data

over different databases in the cloud hardens the cloud against the different form of attacks. Zhang (2018), proposes a hybrid technique for data integrity and confidentiality which uses both authentication techniques and key sharing. The author proposes a three-layered security framework. The first layer is used for authentication using either one-factor or two-factor authentication. The second one is used for data encryption and privacy while the third layer decrypts data to allow for fast recovery of data.

However, effective cloud governance strategies can enable users to realize the cloud's full potential without any data vulnerabilities. The foundation for any cloud security is having visibility in the network. This can be achieved by monitoring the services applied throughout the organization and creating an effective plan to secure their usage. Also, organizations should comply with regulations such as PCI-DSS, EU-GDPR and HIPAA-HITECH. When implementing data loss protection tools, enterprises should ensure that companies have the same set of policies protecting their on-premises data also enforced to data in the cloud. This can be achieved through avoiding sharing sensitive data with unapproved third parties, avoiding upload of high-value information to the cloud, discovering who has access to sensitive data and applying data loss protection (DLP) policies across all cloud services. Aside from cloud best practices, the following tools can be indispensable in providing an additional layer of security: cloud firewall, cloud web gateways, user access control, and cloud access security brokers which provides activity monitoring for cloud services.

A recent report from Kaspersky Lab indicates that at least half of organizations that use cloud services lack a clear understanding of where their data resides. The report also established that most enterprises think that once they migrate to cloud platforms, cloud security becomes solely the responsibility of the cloud service provider, but the reality is that a joint effort between enterprises and cloud service providers is what guarantees the security of data in the cloud. There is no doubt that security in the cloud is a shared responsibility. Rittinghouse & Ransome (2016), opines that the first step in securing a cloud storage is to make sure that only the right individuals have access. An ideal way of controlling access is using identity and Access Management(IAM) permissions. Using IAM, IT managers can control access to critical information in the cloud, which lets administrators access systems or data based on roles of individual users within the enterprise.

Organizations require proper governance to ensure its assets are well implemented and are in line with its standard policies. The assets should be properly maintained and controlled to ensure that they support the strategies and business goals of the organization. In the modern cloud computing, the organization's IT team is not guaranteed to get total control over the provisioning, de-provisioning, and operation of the infrastructures. The lack of full control has increased difficulty for the IT teams in providing governance, compliance and managing the possible risks (Ali, Khan, & Vasilakos, 2015). The teams have had to adopt the traditional governance and control processes to mitigate the potential uncertainties and dangers associated with cloud computing. The effect has led to an evolution in the roles of the Central IT teams. The central IT in collaboration with business units has increasingly played an essential duty of selecting, brokering, and governing cloud services. Third-party providers of cloud management have emerged and are progressively supporting best practices and providing governance.

Moving of an organization to the cloud makes it dependent on the service provider. The performance of its BI gets tied to that of the service provider during a falters (Ali, Khan, & Vasilakos, 2015). If the service provider is down, the organization gets down too. In the past years, cloud players have experienced outages. The providers may lack right processes in place and fail to alert the organization whenever an issue arises. Cloud services need a regular monitoring and supervision of its performance to ensure dependency.

Real-time data is imperative to the data-driven organizations. Due to the reduction in control that is brought by cloud computing, companies may get real-time monitoring issues if the SaaS provider has no policies on real-time monitoring. Such SaaS providers are unable to mitigate these issues.

From the start of cloud computing, security was the primary and valid concern. Organizations are unable to know where their data is processed or stored. The Cloud Security Alliance admitted that Advanced Persistent Threats (APTs) is a danger to cloud computing security. The parasitical cyber-attack can infiltrate systems and establish foothold in the targeted company's IT infrastructure where they can access unauthorized data. APTs slowly pursue their goals as they adopt security measures meant for defense against them. They can move through the data center networks and conjoin it with normal network traffic to achieve their goals. In the cloud, systems from various companies have access to shared memory and are placed close to each other- creating an attack interface. Attackers can use exploitable bugs in programs to infiltrate systems and steal data, giving themselves superuser privileges or alter service operations. Bugs within the operating system can put the security of the whole service or data at risk. In the near past, the sector of cloud computing experienced numerous cyber-attacks. This increased distrust in cloud computing. The cloud service providers have improved the security continuously. Most SaaS providers have implemented secure user identification management, authentication, and controlled access mechanisms. The providers have gotten strict on data recovery policies. For security purposes, organizations are required to comply with regulations and standards (Ali, Khan, & Vasilakos, 2015). Compliance is paramount and should be considered regardless of where the data is stored.

Organization systems may be tampered with if the service provider fails to protect their portion of infrastructure- physical access to their system during maintenance. The cloud can compromise multiple systems. Subscribers are expected to trust their service provider's security measures, but this is limited.

Incompatibility issues may arise between service providers should an organization choose to migrate from one vendor to another. Service providers often create sticky services – systems that are difficult for the end user to transport from one cloud vendor to another. Example, the Blue cloud of IBM is incompatible with Simple Storage System of Amazon.

On the cloud, an organization can experience packet sniffing. Attackers can listen to the raw network for the packets that interest them. The software can then log the data in a file and leak out private data. Providers like Amazon EC2 do not offer protection against a customer's malicious advents to listen to others'.

Additional security implementation has been advised by Cloud Service Association. Organizations should use authenticated encryption to encrypt their data before uploading it to the cloud. The cloud provider further encrypts the encrypted file. The method allows storage of encrypted data and additional metadata that notifies the user of any changes in the file. The security measure protects the organization from malicious users who take advantage of cloud services and could edit shared files.

Lack of resources/expertise has been ranked as the biggest challenge in cloud computing (Ali, Khan, & Vasilakos, 2015). There has been an increase in the workloads placed in the cloud by organizations whereas technology is continually advancing rapidly. These factors are giving organizations tough time keeping up with the tools. Hiring cloud specialists to the IT teams of organizations is prohibitively costly. There is a growing need for expertise. This challenge can be reduced by regularly training IT and development staff. Promoting a strong CIO to champion adoption of cloud can be of good importance. Organizations should turn to automated specialist DevOps tools like Puppet and Chef to monitor the patterns of usage for resources and automate system backups at predefined periods. Such tools have helped in the optimization of governance, security, and cost.

Various cloud service providers have worked to ensure client data is safe and well stored in the cloud. Information about data location centers is kept secret. Data sanitization in the cloud services follows well laid policies that protect the privacy of the organizations. When a storage device reaches the end of use, procedures by AWS that ensure a process that a device is decommissioned are followed in order to prevent client data from being disclosed to unauthorized persons. As directed in the National Industrial Program Operating (NIPO) manual AWS employs the technique DoD 5220.22-M to destroy the data in the process of decommissioning.

Client security has been beefed up by the use of SAML (Security Assertion Markup Language) which uses the XML format to communicate authentication, authorization and attribute data among clients online. It creates a secure platform for businesses to send and receive assertions among partner groups regarding roles, identity, and entitlement of a principal. SAML is used to standardize queries and responses which have entitlement, authentication and attributes information in the XML format. The XML format could be used to request secure user credentials of a user from the SAML authority- asserting party. An asserting party offers a platform where security details can be relayed. The security information is received by a partner site which can either be the requesting party, relying party or the assertion consumer. The transmitted information contains an individual's authentication status, access authorizations and attributes information.

Cloud services employ SSL (Secure Socket Layer) and TLS (Transport Layer Security) which are secure cryptographical protocols. TLS and SSL are designed to provide data integrity and security over the TCP/IP communications. Segments of the network connections are encrypted by the TLS and SSL at the transport layer. TLS protocol allows a safe client-server communication across networks since it is designed to prevent message forgery, tampering, and eavesdropping. It ensures endpoint authentication and uses cryptography to ensure confidentiality. The server gets authenticated because its identity is already known to the client. TLS supports bilateral security in connections where both ends in a connection can be verified through mutual authentication. TLS

ensures safety to user data in the clouds since it prevents data exchange unless authentication is approved and protects against malicious eavesdropping.

Cloud service providers have improved on cloud backups and secure disaster recovery equipment to ensure the safety of client information. Cloud vendors like GIS Cloud offer comprehensive API (Application Programming Interface) which allow companies to perform full backups of all the data they have uploaded to their platform. GIS Cloud has their is regularly updated and is available for restoration when a need arises.

Conclusion

Building security in-house can be a daunting task. Data security concerns are inherent in legacy systems as well as cloud storage platforms. However, many people still view the cloud as innately insecure and riskier although it has the prospect of offering a safer environment when proper security measures are implemented. Hardening cloud systems using a three-layered approach can go a long way in ensuring the security, privacy and integrity of user data.

References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 523-536.

Khan, S. S., & Tuteja, R. R. (2015). Security in cloud computing using cryptographic algorithms. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(1), 148-155.

Lustgarten, S. D. (2015). Emerging ethical threats to client privacy in cloud communication and data storage. *Professional Psychology: Research and Practice*, *46*(3), 154.

Muppidi, S. R., Bird, W. A., Iyer, S. R., Kumar, A., & Nagaratnam, N. (2016). *U.S. Patent No. 9,444,819*. Washington, DC: U.S. Patent and Trademark Office.

Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In *Computational Intelligence and Networks (CINE), 2015 International Conference on* (pp. 116-123). IEEE.

Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: implementation, management, and security*. CRC press.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing. *Computer Communications*, *107*(C), 30-48.

Wall, M. (2016). *Can we trust cloud providers to keep our data safe?* [online] BBC News. Available at: https://www.bbc.com/news/business-36151754 [Accessed 15 Jun. 2018].

Zhang, H. (2018). *How secure is your data when it's stored in the cloud?*. [online] The Conversation. Available at: https://theconversation.com/how-secure-is-your-data-when-its-stored-in-the-cloud-90000 [Accessed 15 Jun. 2018].