5/5/2021

Cloud Technology’s Risk Assessment

Murt Sayeed

CSO 116 – SPRING 2021 TUFTS UNIVERSITY

Abstract:

Over the last two decades, many organizations have utilized cloud technology to modernize their core strategy, while individual consumers have used it for convenience. There is a vast amount of services that the cloud has helped with thus far, such as storing data, scale internal services, or simply using for its computing power. However, little can be said about the risk of cloud technology. This paper will explore the risk assessment of cloud technology as it pertains to internet space and cyber security phenomena. Many cloud companies - such as AWS, Azure, Google and many others - are offering cloud-based applications to their clientele as a SaaS, but what are the security risks and what can we do to mitigate them? Web-based applications are used to access the cloud, but these web-based applications may include their own vulnerabilities. Furthermore, with an abundance of user data used by organizations, who's responsible for information hijacking? In an attempt to answer the above questions, we can better understand cloud technology's security risk and take further actions to mitigate these risks in accordance with the CIA triad.

Table of content:

Introduction:

Cloud industry has become significantly huge in last two decades and it's not going anywhere. Currently, the cloud seems to be more in demand than internet. The cloud provides computing or storage power on an off-site hosted location, as opposed to a local machine. This enables on-demand computational and storage resources with lower economic benefits and an effective way to manage capital expenditure and operational costs. Whether its related to innovation such as self-driving vehicles or grocery shopping at Wholefoods, it has some if not all elements of cloud, which we will find out in this paper. While the word 'cloud' has become popular among organizations, everyone realizes its risk and security measures. Around the globe, the cloud has changed re-defined the way organizations run their business and nobody is denying it. The purpose of this research paper is to look at the holes in security within cloud infrastructure. Assessing the security risk of the cloud should be at the forefront of its usage, whether we are a multi-billion dollars company delivering products and services to our clients, or a university student using the cloud for everyday storage for assignments.

With increased crime in cybersecurity in the internet space, cloud is a familiar face to all the fraudsters. The three main deployment options within cloud start with private, public or the hybrid between the two [15]. Cloud computing has three main services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [16]. We will dive into these individually to gauge their risk landscape since each of these service offers different levels of control and usage. While most cloud services mentioned offer flexibility, pay-per-use preferences, low cost, and automation, security is still an important aspect of its existence. When we delete files or information stored in bytes format in a cloud capacity, people are usually unaware of what happens to it afterwards. Assuming our deleted information is permanently gone and isn't accessible again, stated by our cloud provider, how confident are we in their capability?

Background Information:

Firstly, we must understand what it means to store our information remotely. The information can be stored anywhere inside a country on the servers in virtual machines, where clients may be unaware of the location of their data or computing power location. There is always a possibility of duplicating such information by cloud providers to re-assure clients' data safety. There are many components of the cloud, which are briefly described below at a high level. There are data centers or servers where cloud computing or information is stored via virtual computers. Then we have virtualization, where it can provide the multi-tenancy of cloud-computing by way of scalability and shared resources among its clients [3]. Cloud also includes 'Application Programming Interfaces' (APIs), to communicate between cloud service and local client's application via URL [3]. Last and the most important part is security where encryption is needed to protect information from outside hackers [3].

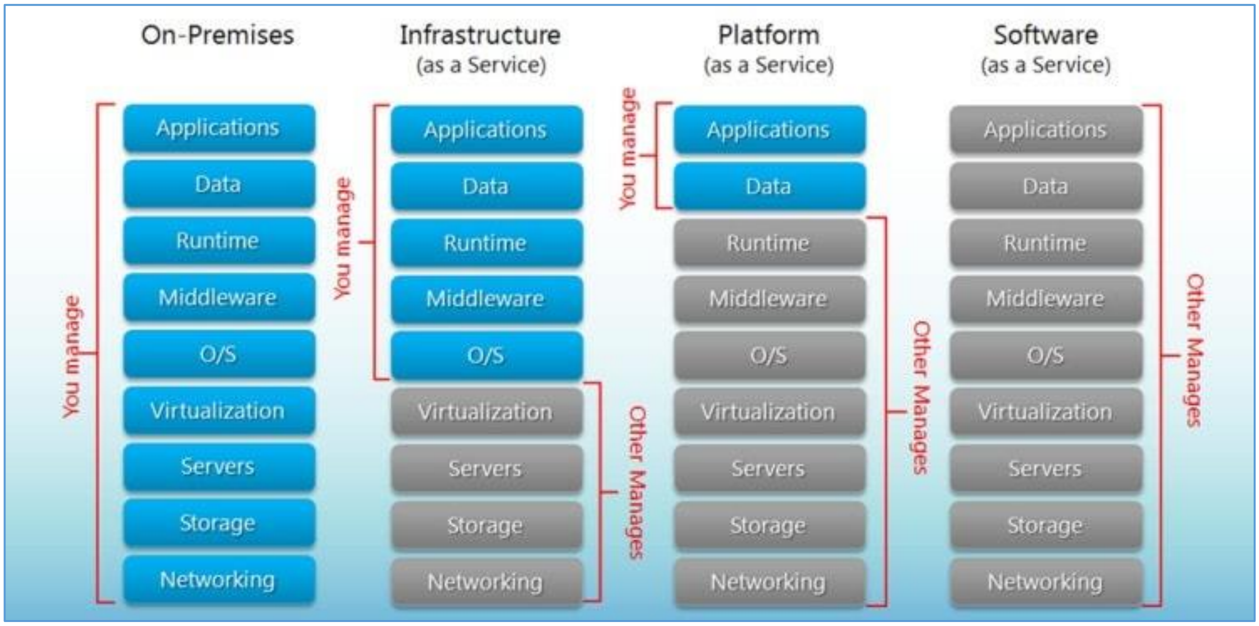
To the Community:

Cloud is the future of technology and it will remain for a couple generations, or at least a few decades. With over 90% of enterprises in US using cloud and spending millions of dollars every year on cloud [1], it is extremely important to understand some of its vulnerabilities. Apple company, as a one cloud service provider, has around 850 million iCloud users as of 2021, with 150 millions of them paid users [2]. Only some of those millions of users know the risk associated with the services they are using. Whether it's about companies' high profits, gaining market share, building innovation or simply using cloud due to ease factor, cloud is touching the lives of many people and we must evaluate its risky nature.

Discussion:

1. Cloud Services – Associated Risks

Our business model or individual needs can tell us lots about what kind of cloud services we would like to have. With such services, all come with some risk and challenges but also a great add-on for us so we can focus on what's more important. The top three cloud delivery models are infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) [4].



Hou, T. (n.d.). IaaS vs PaaS vs SaaS: What you need to know + examples (2018). The BigCommerce Blog.

1.1 Infrastructure as a Service (IaaS)

This service provides virtual machines for many purposes such as data storage, servers, networking capabilities and computing power [4]. The cloud service provider is managing real estate space and hardware to run these giant machines. In addition, the same provider will most likely be responsible for security of such machines used by us and millions of other clients. We are only responsible for the bill on such service by utilizing computing and consumption.

As with any service or product, even IaaS can have security breaches that can become a risks. There is a large possibility that the security challenges on IaaS isn't under our prevue but we may still be affected. Some of the security risks that are under our control can be a huge life saver when it comes to exposing customer's information or dealing with regulatory committees [13]. We must understand, confront and adopt the difference in many vulnerability that come with cloud environment versus on-premises. Otherwise, fraudsters can utilize these points of vulnerability to their advantage. As a client to cloud service, our staff must configure IaaS accurately with proper security standards to avoid unauthorized access [5]. From a cloud service provider, there must be a full control in place on the server's physical environment and not to give full authentication to any one person [5], whether its maintenance or operational staff. Furthermore, security can become complex when the server usage has expanded beyond physicality. As a client, we have to access IaaS among many data centers that can cause additional firewall and routing rules on internet traffic [5], meaning more points to breach security.

1.2 Platform as a Service (PaaS)

This service gives capability to build software on a cloud based platform [4]. The cloud service provider gives us the framework and we manage software applications, while it manages servers, storage and networking [4]. There is a possibility that our platform and what we have built on it may not work if the cloud services provided to us are rendered unexpectedly.

Similar to IaaS, PaaS can also suffer from vulnerabilities. One of the major security risks is not having proper permissions to data stored [7]. Out of the many information leakages in the industry, the fraudsters' ability to access information easily was the most common. Another way for security disasters to happen is using default configurations at the time of initial setup[7]. The security configuration is just as important as marketing products to clients. At the age of internet, another major threat to PaaS is SSL based attacks. This could happen by spoofing SSL certificates and by being a Monkey In The Middle (MIM), where all patch work will have to be upgraded to resolve protocol level flaws[7]. The ability of networks to communicate confidentially and still have access remotely is another security risk one has to consider under PaaS [6]. The major access control items here are authentication, authorization and traceability, where fraudsters may impersonate, carry out phishing attacks, brute forces attacks and/or password reset attacks [6].

1.3 Software as a Service SaaS

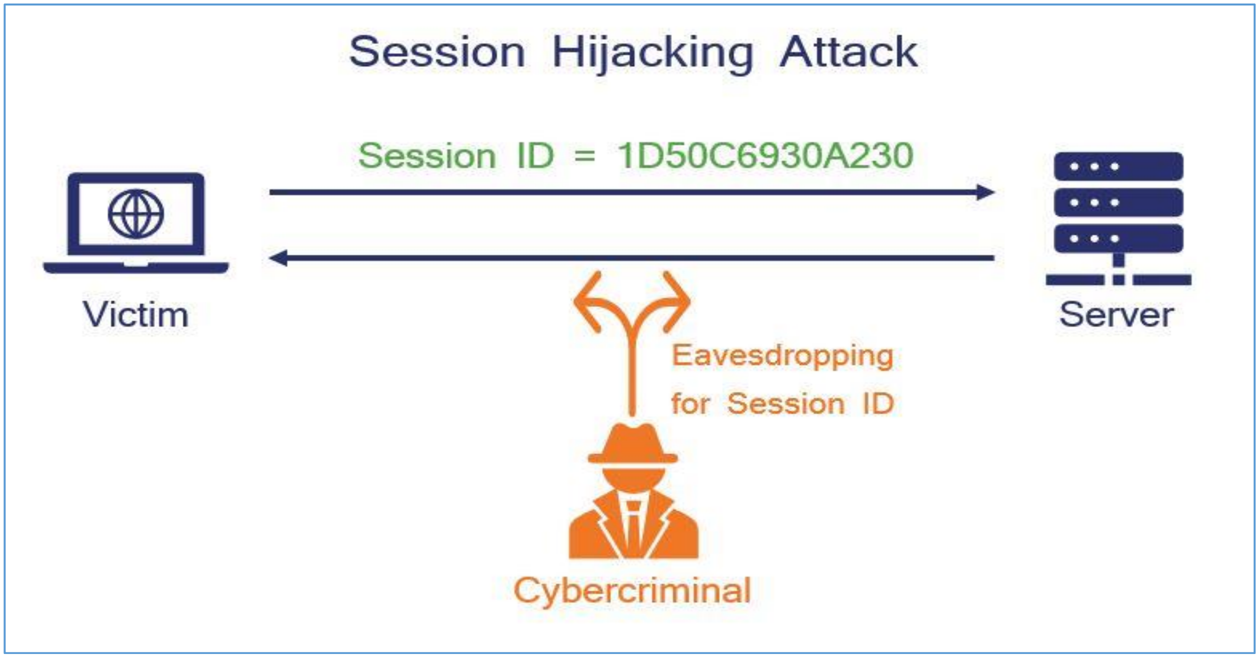
This services, which ready-run software application to its clients, is most common in the marketplace that offers ready-run software application to its clients. Everything else from infrastructure operations to software maintenance of managing, updating and securing are handled by cloud service providers [4], while an application is run through client's browser with no download or installations.

With SaaS taking over cloud industry, many risk factors have also exponentially increased. In 2020, phishing consisted of 90% of cyber-attacks [9]. In addition, it's not uncommon that fraudsters can also take over accounts with the help of employee's credentials, either by some phishing campaign or buy it on dark web via data leaks [9]. Some of these threats can come from within a company since employees end up being the weakest link. As humans, we are accustomed to negligence, whether its weak passwords or lost laptop, fraudster can infiltrate and abuse SaaS information without our knowledge [9]. Fraudsters have also increased their zero-day malware activities where it's hard for us to identify them and a simple auto 'sync' feature on the application could amplify the security threat [9]. According to Bitglass report [9], 44% of scanned organization had some form of malware in at least one of the organization's cloud applications.

2. Web-based Applications – Vulnerabilities and Information Hijacking

We have to utilize web-based applications to get access to anything in the cloud, but are there any vulnerabilities to accessing cloud via web-based applications. Cloud based applications usage is quotidian practice for many of us. These can range from accessing our emails to online banking. While some of these cloud services are state of the art technology to protect in terms of fraudster hacking or hijacking, many are not. The security may not be a priority for these cloud service providers, but as individuals we would like to protect ourselves from any compromised information. One way these fraudsters can have access is through web application's vulnerability.

One of the main risks of such web-based activity is information hijacking [12]. When an individual starts a web session, there is a session ID involved to make any and all requests. A fraudster could take this session ID and pretend to be such individual to access information on the cloud. This vulnerability in cloud can have a great impact on an individual's information.



Vojtko, M. (2020, November 23). The Ultimate Guide to Session Hijacking aka Cookie Hijacking. SecurityBoulevard.

Similar to any crime, there are some breadcrumbs that we can follow. In a web-based session hijacking, most activity happens wirelessly by having access points. A fraudster could hijack such session via scanning and do a sniff attack [18]. There is always a possibility of brute force attack by fraudster to get some IDs stored in a session or cookies [12]. After getting a web session details, fraudsters could spoof MAC address and be a middle person on any communication. This could help fraudsters create their own web session unethically with authenticated individual details, and have access to the cloud service with its information. Above was a simple explanation to understand a fraudster's strategy and better arm ourselves to defend against them and any sophisticated attacks.

Action Items For Us:

1. Cloud Services – Mitigation of Risks

There are many ways to prevent security threats in cloud services. Most responsibilities regarding cloud security fall under cloud service provider, but at the same time client doesn't exactly bypass such security. The most common security issue facing cloud computing is that the client can lose access to the hardware hosting its information. Cloud providers should be responsible to vet their employees while client information and customers are at risk [5]. One important area is the usage of API where the client is responsible for proper utilization of the API while the cloud provider is responsible for its security. As we have a lack of legislative policies in the cloud industry, clients must develop our own robust security policies [13] and make them standard with the service provider as we use their services across international borders.

IaaS is definitely a great to use as long as users are mindful of its security risks. We can train AI take advantage of cloud security and reduce false positives in regards to dangerous malicious attacks. For example, an employee getting access to the server on Starbucks public WIFI might look suspicious via VPN and could be interpreted as fraudster attack. With the help of powerful cloud protection AI, IaaS can help secure our work and information at the same time.

To mitigate PaaS security concerns, we have to take advantage of two things: design application with security as a priority and user authentication prior to using. Therefore, a company is able to create effective information protection strategies and grant access based on application usage. The 2-factor authentication in smart cards and biometric mechanisms can help protect the information from fraudsters. With the help of cloud provider, companies can mitigate risk threats in a timely manner by following correct provider based configuration [7], as Microsoft Azure may have different patches compare to AWS.

The spike in SaaS usage around the industry and continuous technological advances have made this cloud service very receptive to security risks. For larger companies, Cloud Access Security Brokers (CASB) is a viable solution providing visibility [9], access control and data protection using a gateway, proxy or APIs. Due to complexity and cost associated with CASB, smaller companies can use SonicWall Cloud App Security (CAS) to help with data protection for SaaS applications [9]. These additional services can help with security and protect against phishing attacks, email spam, zero-day threats, data loss and account takeovers [9]. With the help of such services, we can achieve our goal to protect company's SaaS landscape and implement robust policies across all cloud services.

2. Web-based Applications – Mitigation of Risks

With cloud recently gaining popularity, it is imperative that web applications are protected. For basic security measures, each cloud based web application must have authentication. In the event of a breach, users must be notified which information was compromised and by who.

We could look at MAC sequence numbers and packet sniffers to check for ARP updates. Since everyday individuals aren't sufficiently educated in cybersecurity to investigate out how a fraudster accessed web-based applications and hijacked information, we will have to come up with common defenses to this risk.

On the cloud service side, we have multiple options to protect ourselves. A combination of HTTP and SSL protocol layers is called HTTPS which can help encrypt communication via secure internet link [14]. This will prevent fraudster sniff and/or steal session ID from the start of the web session. Another way to prevent fraudster from carrying out a brute force attack is One-Time Cookies (OTC) which assigns each web session within an individual browser application [10]. As a client to a cloud service, we also have some options available to ourselves. There are many software available in the market, such as Veracode [8], that can detect against Cross-site scripting (XSS) so we can fix such mistakes on our webpages. The XSS is a pretty common practice for a fraudster to hijack a web session by inserting malicious coding. Another way an individual can help himself by using a secure private network. Public networks, such as airport or Starbucks, are prone to vulnerabilities. Definitely, these practices should provide multiple layers of security to manage cloud's risk. Most if not all, cloud services were using HTTPS in all their web sessions, which is a great news as a user of such service.

Conclusion:

Cloud is a very powerful tool with many different dimensions of risk. With the current growth and security risk associated with cloud, we must better equip ourselves with clear guidance and action plans. Knowing such risks is a good place to start and work towards all security gaps to reduce any conflicts between a cloud service provider and its clients. The service provider that has capabilities in IaaS, PaaS, SaaS, must owe its clients robust security measures that leads to a trusting and long-lasting relationship. A web application access to a cloud service is just as important for its clients as detecting and fixing cyber hijacking. In conclusion, both parties of cloud service must realize the importance of protecting information and must invest in defense strategies against vulnerabilities that are commonly exploited by fraudsters.

References:

[1] Luxner, T. (2021, March 15). Cloud computing trends: 2021 state of the cloud report.
Flexera Blog. https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

[2] Novet, J. (2018, February 14). The case for Apple to sell a version of iCloud for work.
CNBC. https://www.cnbc.com/2018/02/11/apple-could-sell-icloud-for-the-enterprise-barclays-says.html

[3] Vadapalli, P. (2021, February 5). 9 components of cloud computing architecture you should know about.
upGrad blog. https://www.upgrad.com/blog/components-of-cloud-computing-architecture/

[4] Hou, T. (2020, January 9). IaaS vs PaaS vs SaaS: What you need to know + examples (2018).
The BigCommerce Blog. https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-key-differences-between-on-premise-saas-paas-iaas

[5] Henderson, R. (2019, July 30). 8 IaaS cloud security challenges you should be aware of.
Lastline. https://www.lastline.com/blog/8-iaas-cloud-security-challenges-you-should-be-aware-of/

[6] Reddy, P., Bhupathi, V., & Sravan, C. (2017, April). Survey on Security Issues in Platform-as-a-Service Model.
International Journal of Computer Science and Mobile Computing. https://ijcsmc.com/docs/papers/April2017/V6I4201799a12.pdf

[7] Cox, P. (2009, December 11). Top threats in a PaaS cloud service and how to avoid them.
SearchCloudComputing. https://searchcloudcomputing.techtarget.com/tip/Top-threats-in-a-PaaS-cloud-service-and-how-to-avoid-them

[8] Cross site scripting vulnerability. (n.d.).
Veracode. https://www.veracode.com/security/cross-site-scripting-vulnerability

[9] Emmons, S. (2019, September 16). 7 key security risks to address when adopting SaaS applications.
SonicWall. https://blog.sonicwall.com/en-us/2019/09/7-key-security-risks-to-address-when-adopting-saas-applications/

[10] Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. (n.d.). One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens.
Georgia Institute of Technology. https://smartech.gatech.edu/bitstream/handle/1853/42609/GT-CS-12-02.pdf

[11] Vojtko, M. (2020, November 23). The Ultimate Guide to Session Hijacking aka Cookie Hijacking.
SecurityBoulevard. https://securityboulevard.com/2020/11/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/#:~:text=What%20is%20Session%20Hijacking%3F,re%20logged%20in%20and%20authenticated.

[12] Eati, P. (n.d.). 10 most common web security vulnerabilities.
Guru99. https://www.guru99.com/web-security-vulnerabilities.html

[13] Conradi, M. (2014, August 29). Managing legal risks arising from cloud computing.
Technology's Legal Edge. https://www.technologyslegaledge.com/2014/08/managing-legal-risks-arising-from-cloud-computing/

[14] Lukan, D. (2015, November 20). Security vulnerabilities in cloud applications.
Infosec Resources. https://resources.infosecinstitute.com/topic/security-vulnerabilities-in-cloud-applications/

[15] MORROW, T. (2018, March 5). 12 risks, threats, & vulnerabilities in moving to the cloud.
SEI Blog. https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

[16] 7 cloud computing security vulnerabilities and what to do about them. (2020, July 13).
Cypress Data Defence. https://towardsdatascience.com/7-cloud-computing-security-vulnerabilities-and-what-to-do-about-them-e061bbe0faee