A Literature Based Study on Cyber Security Vulnerabilities

ROSHINI SOWRIRAJAN
Senior Systems Engineer, Infosys
Email: roshvinisowrirajan@gmail.com

Abstract: **Cloud computing has emerged from the legacy datacentres. Consequently, threats applicable in legacy system are equally applicable to cloud computing along with emerging new threats that plague only the cloud systems. Traditionally the datacentres were hosted on-premises. Hence, control over the data was comparatively easier than handling a cloud system which is borderless and ubiquitous. Threats due to multi-tenancy, access from anywhere, control of cloud, etc. are some examples of why cloud security becomes important. Considering the significance of cloud security, this work is an attempt to understand the existing cloud service and deployment models, and the major threat factors to cloud security that may be critical in cloud environment. It also highlights various methods employed by the attackers to cause the damage. Cyber-attacks are highlighted as well. This work will be profoundly helpful to the industry and researchers in understanding the various cloud specific cyber-attack and enable them to evolve the strategy to counter them more effectively.**

Key words: **Cloud Computing; Data Centres; Cyber Attacks; Multi Tenancy; Cloud Service;**

INTRODUCTION

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware. **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed. **Information security** protects the integrity and privacy of data, both in storage and in transit. **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella. For various types of attacks, one may refer to the articles listed under references.

The major goal of cloud computing is to reduce the operating cost, increase throughput, increase the reliability and availability[1]. Outsourcing of technical resources enables the organization to concentrate on business need, instead of technical aspect that is managed by the experts in Information Technology area. To facilitate such users, a web based paradigm known as cloud computing has emerged and offering the services on utility model[2]. Cloud computing has emerged from the legacy datacentres and so, the threats from legacy system are applicable for any cloud based system, along with emerging new threats that plague only the cloud systems. Traditionally the datacentres were hosted on-premises. Hence, control over the data was comparatively easier than handling a cloud system which is borderless and ubiquitous. Threats due to multi-tenancy, access from anywhere, control of cloud, etc. are some examples of why cloud security becomes important**.** Considering the significance of the cloud models, cloud security is an important factor to think about. This review paper, gives an idea on the existing cloud models and various cyber threats, and attacks the system has undergone.

I. CLOUD SERVICE MODELS

1. INFRASTRUCTURE AS A SERVICE (IaaS)

Infrastructure-as-a-Service (IaaS) can be defined as the use of servers, storage, and virtualization to enable utility like services for users. IaaS eliminates the capital expense of building the internal infrastructure. An IaaS provider manages the physical edge of the infrastructure (servers, data storage space, etc.) in a data center, but allows customers to fully customize those virtualized resources to meet their specific needs. Hence, security is a big concern within IaaS, especially considering that the rest of the cloud service models run on top of the infrastructure and related layers [6].

Examples of IaaS: Microsoft Azure, Amazon Web Services (AWS), Cisco Metacloud, Google Compute Engine[8].

2. PLATFORM AS A SERVICE (PaaS)

Platform-as-a-Service (PaaS) providers offer access to APIs, programming languages and development middleware which allows subscribers to develop custom applications without installing or configuring the development environment[6]. In PaaS, development environment is offered as service. It is extremely useful for any company that develops web-based software and applications. Many of the tools required to develop for multiple platforms (computers, mobile devices, browsers, etc.) can be quite expensive. So, customers can access the development tools using PaaS cloud service[9]. But, they do not have the assurance that the development environment tools provided by a PaaS provider are secure, because customers do not usually have access to the underlying layers.

Examples of PaaS: AWS Elastic Beanstalk, Apache Stratos, Google App Engine, Microsoft Azure[8].

3. SOFTWARE AS A SERVICE (SaaS)

Software-as-a-Service (SaaS) gives subscribed or pay-per-use users access to software or services which reside in the cloud and not on the user's device[6]. In Saas, applications are offered as service. SaaS applications allow businesses to get up and run quickly, and scale operations quickly. You do not need to purchase or implement the hardware and software used to deliver your business services[9]. With Saas, the burden of security lies with the service providers because the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility.

Examples of SaaS: Microsoft Office365, Google Apps, Cisco Webex[8].

4. FUNCTION AS A SERVICE (FaaS)

Function as a service (FaaS) is a cloud computing service that allows developers to build, compute, run, and manage application packages as functions without having to maintain their own infrastructure. It simplifies the runtime resource management of cloud applications and enables fine-grained scaling and billing at the function level, thus becoming the most widespread serverless paradigm today[7].Customers only pay for the resources they use, making FaaS the truest form of "pay-as-you-go" cloud computing. Most FaaS applications are quite simple and can be deployed very quickly. The cloud customer just needs to upload the compiled function code and tell the platform how to provision resources when it executes[9]. Cost-effective use of FaaS entails appropriately deploying individual functions[9]. For large FaaS applications, strong process and operational controls combined with automation are necessary to provide reasonable assurance of application security during the development and deployment process. Without these controls, particularly in DevOps/continuous development environments, maintaining security can be problematic. FaaS application implementations are typically subject to OWASP vulnerabilities and require corresponding security controls[19].
Examples of FaaS: AWS Lambda, Azure Functions[8].

II. CLOUD DEPLOYMENT MODELS

1. PUBLIC CLOUD

A public cloud is a subscription service, that is offered to all the customers who want similar services. The service provider owns and operates all the hardware necessary to run a public cloud. Vendors keep the devices in massive data centres. Its virtual environment is inexpensive and can be easily configured and quickly deployed, making it perfect for test environments[10]. It is a multi-tenant environment. Multitenancy exploits may allow one tenant or hacker to view all the data or assume the identity of another client.

2. PRIVATE CLOUD

A private cloud belongs to a specific organization. That organization controls the system and manages it centrally. While a third party (for example, a service provider) can host a private cloud server, most companies choose to keep the hardware in their local data center. From there, an internal team can oversee and manage everything[10]. Most organizations do not have the same physical security, provided by third-party data centers, which may make their data vulnerable to various threats.

3. HYBRID CLOUD

A hybrid cloud is a combination of private cloud and public cloud. Generally, a hybrid cloud starts out as a private cloud, which then extends the integration to use one or more public cloud services. This deployment model is used when companies have sensitive data that cannot be stored in the cloud or regulatory requirements that call for data protection, storage, and more[11]. Data flowing between public and private clouds create vulnerabilities that may lead to eavesdropping or cyberattacks.

4. COMMUNITY CLOUD

A Community cloud provides services to a community of users or organizations with shared interests or concerns. Organizations using this cloud service have shared missions, governance, security requirements, and policies. Cloud services can be hosted on the premises of the consumer organization, on the premises of the peer organization, at one provider, or a combination of these [11]. Although the physical existence of the shared cloud may reside on any member's premises, or even on a thirdparty site, managing the community cloud may become complicated, due to unspecified or shifting ownership and responsibility, making it somewhat technically challenging to deal with concerns over resource management, privacy, resilience, latency, and security requirements.

III. POSSIBLE CYBER ATTACKS IN CLOUD MODELS

1. PHISHING

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Phishing through e-mail deception (e-mail spoofing) or immediate messaging guides victims to access a counterfeit website whose appearance and impression are practically indistinguishable to the authentic one[14].

2. HACKING

Hacking is the gaining of access(wanted or unwanted) to a computer and viewing, copying, or creating data(leaving a trace) without the intention of destroying data or maliciously harming the computer. Hacking and hackers are commonly mistaken to be the bad guys most of the time. Crackers are the ones who screw things over as far as creating virus, cracks, spyware, and destroying data. A hacker first attacks an easy target, and then uses it to hide his or her traces for launching attacks at more secure sites[13].

3. DISTRIBUTED DENIAL OF SERVICE

The DDoS attack will send multiple requests to the attacked web resource, with the aim of exceeding the website's capacity to handle multiple requests, and prevent the website from functioning correctly. An explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services[13].

4. VIRUS DISSEMINATION

A virus is a program that can 'infect' other legitimate programs by modifying them to include a possibly 'evolved' copy of itself. Viruses can spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. Computer viruses currently cause billions of dollars worth of economic damage each year[14].

5. PASSWORD ATTACKS

The attack where hackers attempt to access a file, folder, account, or computer secured with a password leading to data breach. As one of the most common application security threats, password attacks accounted for more than 81% of data breaches in 2022. Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking passwords[13].

6. SPAMMING

Spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately. The most widely recognized form of spam is e-mail, which may have original content with phishing URLs to steal useful data. This kind of email is just spam[15]. Similar abuses in other media are instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, social spam, television advertising and file sharing spam[14].

7. WORMS

Computer worms are a type of malware that have a complex technological structure and the ability to automatically create replicas of themselves without human interaction and distributing themselves to other computers connected to the network; they have a malicious code component that allows them to infect one computer and then use it to infect others. This cycle repeats itself, rapidly increasing the number of infected computers if action is not taken in time[16].

8. SNIFFING ATTACK

A sniffing attack occurs when an attacker uses a packet sniffer to intercept and read sensitive data passing through a network. Common targets for these attacks include unencrypted email messages, login credentials, and financial information.Despite being supposedly a simple task, it could sometimes be a highly resource consuming process[17].

9. HONEYPOT ATTACK

Honeypot, also known as Intrusion Detection Technology, is a type of security technology that screens devices to prevent unwanted activities. It is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems[18].

10. SQL INJECTION

SQL injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box. Web application vulnerability is one of the major causes of cyber-attacks. Cyber criminals exploit these vulnerabilities to inject malicious commands to the unsanitized user input, in order to bypass authentication of the database[21].

IV. CONCLUSIONS

Several organizations and working group are putting their efforts to strengthen the security in cloud computing. Although various study reveals that hosted model is more secure relative to the on-premises cloud model, many attacks are targeting the hosted model to exploit the vulnerabilities. DDoS and Phishing are the major method employed to attack the cloud. Finally, in the light of phishing and DDoS attack that took place in many of the cloud revealed, it can be concluded that they are causing huge financial losses, damage to privacy of

data. Although a number of solutions are existing that are countering various attacks, still there is further need to strengthen the security in hosted as well as on premises cloud, in order to restore the confidence of users.

V. FUTURE SCOPE

Currently, traditional laws and technical protection are no longer enough against computer crimes. Growth of cybercrimes shows that there is a high chance that it would continue growing. Cyber criminals always come up with a new way of committing the crimes. Authorities must increase the skill levels to catch up with cybercrime offenders. Cybercrime has an unpredictable future judging from the trends where they always end up a step ahead of the authorities. And so, there is a need to further investigate the current status of cybercrime.

ACKNOWLEDGEMENTS

I hereby convey my sincere thanks to Dr.Sridhar Seshadri, Ex.Vice-Chancellor, currently CEO, Sbyte Technologies for his continuous support, guidance and mentorship. His comments while reviewing this paper for publication are highly appreciable and well taken to modify this final version

REFERENCES

[1] A. Hall, “Recent phishing attack targets select Microsoft employees”(accessed on 24 Jan 2014) available at

https://blogs.technet.com/b/trustworthycomputing /archive/2014/01/24/post.aspx (accessed on 01 Feb 2014).

[2] B. Hayes, “Cloud computing”, Communications of the ACM, vol. 51, no. 7, 2008.

[3] D. Marcus, D. and R. Sherstobitoff, “Dissecting operation high roller”, Mcfee, white paper, 2012, available at http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

[4] B. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall “Cloud computing”, 2009. http://www.ibm.com/developerswork/websphere/ zones/hipods/library.html.

[5] Ericka Chickowski,Sony Still Digging Its Way Out of Breach Investigation, Fallout ,02 Apr 2013, available at

http://www.darkreading.com/attacks-breaches/ sony-still-digging-its-way-out-of-breach/229402823.

[6] Benefits and challenges of three cloud computing service models ref.

https://ieeexplore.ieee.org/abstract/document/6412402/

[7] RDOF: Deployment Optimization for Function as a Service ref.

https://ieeexplore.ieee.org/document/9582257

[8] https://www.vxchnge.com/blog/different-types-of-cloud-computing

[9] Cloud Computing Deployment Models: A Comparative Study ref.

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3832832_code3665699.pdf?abstractid=3832832&mirid=1&type=2

[10] https://phoenixnap.com/blog/cloud-deployment-models

[11] https://crmtrilogix.com/Cloud-Blog/Cloud-Models/ Cloud-D

[12] http://ijeie.jalaxy.com.tw/contents/ijeie-v1-n2/ijeie-v1-n2.pdf#page=29

[13] https://www.researchgate.net/profile/Jehad-Al-Amri/publication/341113435_Cyber_ Attacks_and_Impacts_A_Case_Study_in_Saudi_ Arabia/links/5eaedbf245851592d6b535dd/Cyber-Attacks-and-Impacts-A-Case-Study-in-Saudi-Arabia.pdf

[14] https://www.researchgate.net/profile/Bushra-Elamin/publication/309040131_Cyber_Crime_in_ Kingdom_of_Saudi_Arabia_The_Threat_Today_ and_the_Expected_Future/links/57ff2f9508ae6b2da3c89b36/Cyber-Crime-in-Kingdom-of-Saudi-Arabia-The-Threat-Today-and-the-Expected-Future.pdf

[15] https://ieeexplore.ieee.org/abstract/document/ 7322709/

[16] https://link.springer.com/chapter/10.1007/ 978-3-030-70416-2_7

[17] https://ieeexplore.ieee.org/abstract/document/ 9447699/

[18] Review of Cyber Attack Detection: Honeypot System ref.

https://www.webology.org/data-cms/articles/ 20220123051035pmWEB19370.pdf

[19] https://ieeexplore.ieee.org/document/ 9194431

[20] https://www.ijltet.org/wp-content/uploads/2015/ 08/631.pdf

[21] https://ieeexplore.ieee.org/abstract/document/ 9397066/

