**RIGA TECHNICAL UNIVERSITY**

**Faculty of Computer Science and Information Technology**

**Cybersecurity Engineering**

**Introduction to Cybersecurity  
  
  
Cyber Attacks on Cloud and Machine Learning Solutions**

**Ibrahim Can Kilic**

**Kyaw Min Thant**

**December 2022**

**Introduction to Cloud and Cloud Security**

Cloud computing is continuous delivery of IT operations over the Internet with pay as much as you use the pricing model. By using cloud computing services, users can access, use, develop and manage several technology services such as databases, storage, and computing power. Cloud providers like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Alibaba Cloud, Oracle Cloud, and IBM Cloud (Kyndryl) offer different solutions according to customer needs.

The Covid 19 pandemic has accelerated companies' transition to cloud operations. The need for cloud computing systems is increasing day by day. In last 5 years, The number of cyber-attacks on Cloud services has increased rapidly. Incidentally, cloud cyber-attacks accounted for 20% of all cyber-attacks in 2020, making cloud computing platforms the third most-targeted cyber environment. [1]

Cloud security is designed with technology, protocols, and best practices that protect cloud computing systems, applications, or websites running in the cloud, and data held in the cloud. Cloud security is designed to protect these things; physical networks, data storage, data servers, computer virtualization frameworks, operating systems, middleware, runtime environments, data, applications, and end-user hardware. Securing the cloud can look different based on who has authority over each component, which is important to understand how these are commonly grouped. To simplify, cloud computing components are secured from two main viewpoints: cloud service types and cloud environments.

There are many things to make the cloud more secure. The main thing that we have to do is encryption. Encryption is one of the best ways to secure your cloud computing systems. Another notable way to secure the cloud is configuration. Many cloud data breaches come from basic vulnerabilities such as misconfiguration errors. We can do other things to secure clouds such as using strong passwords, using password managers, back up data regularly, and updating permission. [2]

Cloud vulnerabilities are one of the main parts of cloud security and need to focus on cloud computing mainly. According to the 2021 study by IBM, there are six types of cloud vulnerabilities. The first vulnerability is cloud misconfiguration, which is probably the most common vulnerability that organizations face. Misconfigurations can take many forms and shapes, a few of which are public data storage, using an out-of-date version of SSL/TLS, and using one place secure secret management solution. The second vulnerability is insecure APIs. APIs are proliferating in modern software development, being used in microservices, applications, and website backends. They must handle requests received from mobile devices, applications, webpages, and third parties, as well as bots, spammers, and hackers. This is why having a secure API is critical to ensuring cyber threat mitigation and protecting against unwanted traffic. The third one is the Lack of visibility. As the use of cloud services increases, so does the scale of your infrastructure. When companies are using thousands of instances of cloud services, it can be easy to get lost in them or forget about some of those running instances. Visibility into the state of your entire infrastructure must be easy and convenient to access. The fourth vulnerability is the Lack of multi-factor authentication. Multi-factor authentication (MFA) is an authentication method in which a user must present at least two forms of identification validation to access an account or data. For instance, a typical MFA is when a user has to enter a username and password. The user is then prompted to enter a second validation, such as a one-time password/code received via SMS, email, or push notification on their cell phone. Passwords and users are vulnerable to theft, making a lack of MFA a potentially critical vulnerability. The fifth one is malicious insiders. Unauthorized access occurs when a user obtains access to some or all of your company’s cloud resources. There are a few ways that these malicious insiders can gain access to your cloud accounts. As mentioned in the cloud misconfiguration section, this can result from too loose of rules or a former employee still having valid credentials to the accounts. The final one is distributed denial-of-service attacks. Distributed denial-of-service (DDoS) attacks are malicious efforts to take down a web service such as a website. It works by flooding the server with requests from different sources (hence distributed) and overcharging it. The goal is to make the server unresponsive to requests from legitimate users. [3]

**Top Cloud Attacks in Last years**

**Raychat** is an online chat application and customer support service that enables users to communicate directly with their customers. The company had a large scaled cyber-attack in February of 2021. A cloud database configuration breach gave hackers free access to 267 million usernames, emails, passwords, metadata, and encrypted chats. Shortly thereafter, a targeted bot attack erased the entirety of the company’s data.

**Cognyte** is a company that provides security software solutions and cyber analytics. The company had an unsecured database in May of 2021. The culprits managed to expose 5 billion records. Information such as names, email addresses, passwords, and vulnerability data points within their system was leaked.

**Accenture** is one of the biggest information technology services and consulting company. Accenture had a LockBit ransomware attack in August of 2021. The culprits claimed to have stolen 6TB worth of data, for which they requested a ransom of $50 million.

**Kaseya** is a software company that develops software for managing networks, systems, and information technology infrastructure. In July of 2021, IT solutions provider Kaseya identified an attack on their unified remote monitoring and network perimeter security tool. The attackers aimed to steal administrative control for Kaseya services; from managed service providers to downstream customers. The attack itself disrupted the organization’s SaaS servers and affected on-premise VSA solutions used by Kaseya customers across nearly a dozen countries.

**Facebook** is an online social media platform with around 2 billion daily users. They reported a breach affecting over 533 million user records, which were publicly exposed on Amazon’s cloud computing service in April of 2021. [4]

**Machine Learning Solutions for** **Cloud Security**

Traditional methods for the prevention of threats on the cloud are insufficient due to the increasing number of attacks and attack diversity. Machine learning approaches can offer more responsive and automated security solutions as they handle data more effectively. Machine learning-based systems for the confidentiality and integrity of data in the cloud, the availability of cloud resources, and authentication on the cloud platform are very popular lately. [5]

Intrusion Detection Systems (IDS) is a cyber security system that works as software or hardware designed to monitor a network and detect vulnerabilities and attacks. IDS use comprehensive approaches to protect the information in cloud applications from attacks. The IDS system has functions such as detecting the attacks, reporting and recording of these attacks as evidence in the future and quarantining damaged systems. In addition, it tries to facilitate the detection of future attacks by recording current attacks and attack models.

Intrusion Detection System (IDS) has become the most commonly used component of computer system security and compliance practices that defends network accessible Cloud resources and services from various kinds of threats and attacks. [6] [Intrusion Detection Systems](https://wisdomplexus.com/blogs/different-types-of-intrusion-detection-systems-ids/#DifferentTypes)is classified into 5 types.

* Network Intrusion Detection System (NIDS)
* Host Intrusion Detection System (HIDS)
* Protocol-based IDS (PIDS)
* Application Protocol-based IDS (APIDS)
* Hybrid Intrusion Detection System

Intrusion Prevention System (IPS) is a network security tool. This prevention system is generally created behind a firewall and continuously monitors the network for suspicious activities. IPS prevents the attacks from entering the network by examining various data records and prevention the demeanor of the pattern recognition sensor. When an attack is identified, intrusion prevention block and log the offending data. [7] Intrusion Prevention System (IPS) is classified into 4 types.

* Network-based intrusion prevention system (NIPS)
* Wireless intrusion prevention system (WIPS)
* Network behavior analysis (NBA)
* Host-based intrusion prevention system (HIPS)

The differences between IDS and IPS

* IPS is set up to take action against attacks, but IDS only works to detect.
* IDS and IPS can work in hardware or software.
* IDS and IPS try to detect attacks by comparing known threats and behavior patterns to their databases.
* IPS takes action on its own but IDS reports to the person who will take action. For this reason, there is a need for personnel who constantly monitor the IDS system.
* Both work by being located behind a firewall.

**References**

**[1]** Foundry. 2022. *Cloud Computing Study: Executive summary outlining the 2022 research findings* [Online]. Available at: https://resources.foundryco.com/thank-you-cloud-computing-executive-summary [Accessed: 28 December 2022].

**[2]** Kaspersky. *What is Cloud Security?* [Online]. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security [Accessed: 28 December 2022].

**[3]** Gui Alvarenga. 28 June 2022. *Top 6 Cloud Vulnerabilities*[Online]. Available at: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-vulnerabilities/ [Accessed: 21 December 2022].

**[4]** Cybertalks. 26 April 2022. *Top 5 cloud security breaches (and lessons)* [Online]. Available at: https://www.cybertalk.org/2022/04/26/top-5-cloud-security-breaches-and-lessons/

**[5]** A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

**[6**] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, "A survey of intrusion detection systems for cloud computing environment," 2016 International Conference on Engineering & MIS (ICEMIS), 2016, pp. 1-13, doi: 10.1109/ICEMIS.2016.7745295.

**[7]** D. Stiawan, A. H. Abdullah and M. Yazid Idris, "The trends of Intrusion Prevention System network," 2010 2nd International Conference on Education Technology and Computer, 2010, pp. V4-217-V4-221, doi: 10.1109/ICETC.2010.5529697.