SoK: Assessing Cloud Security

Eman Kumar Saha Student ID: 40303181
Arjun Kumar Saha Student ID: 40256758

Objective

In the present-day server runs from the cloud. It is used much more widely now than a few years ago. Its growing use is directly correlating with its increasing security risk. This project investigates some aspect of cloud security. We pay particular attention to the cloud computing risks, threats and vulnerabilities that may block its increasing use.
Section III dedicates itself to understanding what cloud computing is, how it works, how it became a tenant of the tech industry, and why the tech industry has moved to a cloud computing model. Section II covers our research and the cloud computing security techniques and protocols. In Section III, we begin with the risks and the weaknesses of cloud computing. Section IV demonstrates Attack Tree.

Section: I

What is Cloud computing and what are the types of Cloud Computing?

Traditionally, servers would be deployed into physical data centres and configured for specific needs. But this approach has changed a lot with the arrival of cloud computing. As a result, cloud computing enables users to access resources remotely, providing advantages such as flexibility, scalability, security, and cost-effectiveness over traditional infrastructure.

NIST definition of cloud computing

Cloud Computing is a computing model focused on delivering instantly provisioned and released configurable pools of delivery on-demand of shared computing resources like storage, servers, applications, and network services with minimal management effort or service provider interaction [3]. Cloud computing is generally defined from different perspectives, but for IT users, cloud computing can be defined as the delivery of storage, computing power, and applications over the internet from a centralized data centre. On the development side, it is a big scale development platform and runtime environment. Infrastructure providers and system administrators, meanwhile, view it as a vast, distributed data center architecture interconnected through IP-based networks [2].

There are three primary cloud deployment models:

- Public cloud
- Private cloud
- Hybrid cloud

Additionally, cloud services are typically offered in the following forms:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as Service (SaaS)

Cloud computing is largely driven by the principles of self-service, simplification, standardization, economies of scale, and continuous technological advancement [1].

Do Cloud Computing Resources Actually Come from the Sky? (How Cloud Computing Works)

No, cloud computing resources do not come from the sky. These resources are actually provided through one or more physical data centers that are geographically separated and securely maintained. In the case of private clouds, organizations manage and host their own infrastructure, enabling employees to access systems remotely while ensuring both scalability and security. On the other hand, public cloud providers like Amazon Web Services (AWS), Microsoft Azure, and others offer their own infrastructure to customers. These services are designed to deliver high flexibility, global availability, strong security, and reliable scalability. These providers operate multiple data centers worldwide to ensure service uptime, often achieving up to 99.99% availability. Figure 1 illustrates a general view of how cloud computing operates.

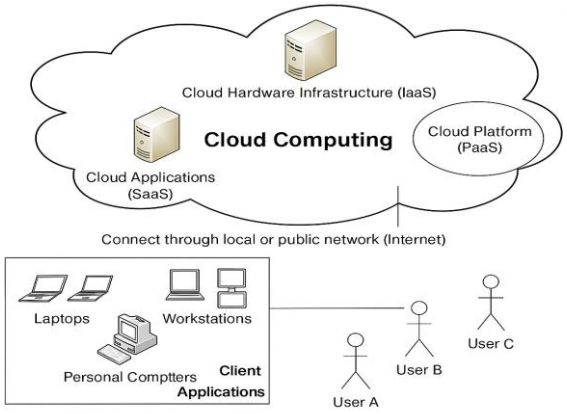

Figure 1:Architecture of Cloud Computing

Why has the Tech Industry shifted towards cloud computing?

Initially, businesses required physical servers to run applications, with each server supporting only one application. The introduction of virtual machines (VMs) allowed multiple applications to share resources on a single server. However, in distributed computing environments, a significant portion—up to 85%—of computing capacity remained unused. Additionally, around 66% of IT spending was focused on maintaining existing infrastructure rather than supporting innovation and new capabilities [1].

The rise of cloud computing has revolutionized this model by eliminating the need for upfront costs associated with physical infrastructure, which has particularly benefited startups by enabling them to deploy and scale applications without large initial investments. Figure 2 illustrates the evolution of technology leading to the adoption of cloud computing.

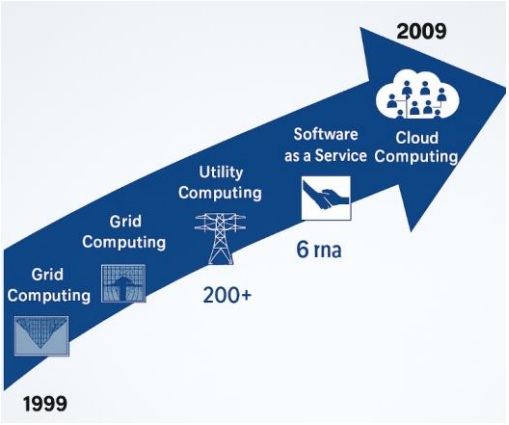

Figure 2: Evaluation of Cloud Computing

Section II: Navigating Cloud Security Essentials

What is Cloud security & the key components?

Cloud computing consists of two main parts: the frontend (or client-side) and the backend, which encompasses the physical infrastructure. These components can be further segmented, but cloud security focuses on securing the entire system, from the host to the end-user [4]. The core objective of cloud security is to integrate policies, procedures, and technological solutions to ensure the protection of data, compliance with regulations, and management of user and device control over privacy, access, and authentication [5].

Which critical components must be secured to ensure a safe cloud environment?

To maintain a secure cloud infrastructure, multiple layers and elements must be protected. Cloud security encompasses a wide range of components, including:

- **Physical infrastructure**: This involves safeguarding the foundational hardware such as routers, power supply systems, cabling, and climate control equipment.
- **Data storage systems**: Devices like hard drives that store critical information must be secured.
- **Data servers**: These are the core units of computing that handle network operations and must be protected both physically and digitally.
- **Virtualization technologies**: This includes securing virtual machine software along with both host and guest systems.
- **Operating systems**: As the base software layer, operating systems require robust security controls.
- **Middleware and runtime environments**: Middleware like APIs and execution environments need to be managed to ensure secure application operations.
- **Data**: All types of data, whether stored, modified, or accessed, must be protected from breaches.
- **Applications**: Common software solutions, from email to productivity tools, must have appropriate security layers.
- **User-end devices**: Endpoints like computers, smartphones, and IoT devices must also be considered part of the overall security framework [6].
- The space that cloud systems occupy is vast; therefore their protection is ruled by core security principles. These guiding concepts are distilled in the STRIDE model and include:
- · **Confidentiality** – proper prevention of unauthorized access to information
- · **Integrity** – the need to ensure that data cannot be changed without permission
- · **Availability** — ensuring systems and data are available when needed
- **Authentication** – confirming the identity of individuals and devices
- · **Authorization** — access rights according to identity and role
- · **Non-repudiation** – guarantee that something that has happened cannot be denied

These principles form the foundation for building a secure and trustworthy cloud computing environment.

Section III: Cloud attack surface

Unauthorized access to cloud-based systems and data presents a serious challenge to information security. These breaches typically stem from weaknesses in authentication and authorization mechanisms, which can be exploited in several ways:

1. **Brute Force Attacks**:
   Attackers use a brute force attack to figure out passwords by trying each possible combination in turn. Current brute force methods utilise sophisticated algorithms—rule-based or masked attacks, for example—to improve the performance of a guess, which in some situations renders even lengthy and complex passwords susceptible to decryption [14].

2. **Credential Stuffing**:
   This method involves using username and password combinations leaked from previous data breaches to gain access to different systems. Since many users reuse passwords across multiple platforms, this technique can be highly effective. Automated tools allow attackers to test thousands of login credentials in a very short time [7].

3. **Exploitation of Default Credentials**:
   Many systems are configured with default login credentials during installation. These credentials are often well-known or easy to find and are rarely updated by users, leaving systems exposed to unauthorized access attempts [15].

4. **Misconfigured Access Controls**:
   Improperly set permissions or access control rules can give users—or attackers—more privileges than necessary. This increases the risk of unauthorized activities, especially when combined with weak or missing authentication methods.
5. **Lack of Multi-Factor Authentication (MFA)**:
   MFA, on the other hand, makes this exponentially more difficult; without it, one compromised factor (eg stolen password) grants complete access to a system. MFA provides additional security, which could be a verification code or a biometric check, virtually eliminating the chances of unauthorized entry [15].

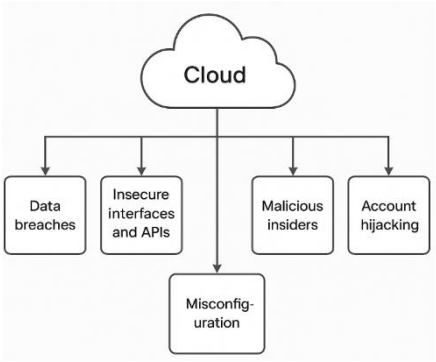

Figure 3: Cloud Attack Surface

Data Breach

Data breaches are a major concern in cloud systems and often arise from flaws in how data is stored or transmitted. Several key techniques used by attackers include:

- **Exposure of API Keys**: Developers sometimes mistakenly embed API keys in publicly accessible code repositories or client-side applications. If communication between servers is not encrypted, these keys can be intercepted and misused [17].
- **Manipulation of API Parameters**: Weak validation allows attackers to alter API parameters, enabling them to access unauthorized data or functions. This can be exploited to tamper with SQL queries or bypass security protocols [18].
- **SQL Injection**: Attackers can inject malicious SQL commands into an application's input fields, giving them the ability to run unauthorized commands against the back-end database to retrieve, modify, or delete sensitive data. [7][8].
- **Cross-Site Scripting (XSS)**: XSS attacks happen when attackers insert malicious scripts into web content that other people view. This is typically a result of not properly sanitizing and validating user inputs [11].

Denial of Service (DoS):
These attacks are designed to disrupt services, making them inaccessible to legitimate users.

- **Distributed Denial of Service (DDoS)**: Attackers flood the target system with massive volumes of traffic from multiple sources, making it hard to block the attack by simply filtering individual IP addresses [8][14].
- **Misconfigured Services**: Incorrectly set up systems—like APIs without rate limiting—can allow attackers to flood them with unlimited requests, making them more vulnerable to service exhaustion [9][10][15].

Elevation of Privilege:
These attacks occur when an attacker escalates their level of access beyond what they're authorized to have.

- **Exploitation of Hypervisor Vulnerabilities**: Attackers can exploit previously unknown flaws (zero-day vulnerabilities) in the hypervisor to gain unauthorized control over virtual machines [16].
- **Escaping from Containers or VMs**: Some attackers target weaknesses in virtualization environments, breaking out from isolated containers or virtual machines to access the host system

or other environments [11].

Account Takeover:
This type of attack involves gaining full control over user accounts, allowing attackers to impersonate users or steal sensitive information.

- **Phishing & Session Hijacking**: Through deceptive emails or fake websites, attackers steal user credentials. They may also hijack active sessions if session tokens are not properly secured [9][13].

- **Flaws in OAuth & OpenID Connect**: Attackers may exploit weak implementations of these authentication protocols, such as redirecting users to malicious websites or failing to validate tokens securely [13]

Cloud Service Misuse:
As organizations increasingly adopt cloud solutions, new threats emerge that exploit cloud features in unintended ways.

- **Unauthorized Resource Usage (Cryptojacking)**: Malicious actors use cloud computing resources without permission—typically to mine cryptocurrencies—causing slowdowns and increased operational costs [12].
- **Shadow IT & API Misuse**: Employees may use unapproved cloud applications, bypassing corporate security controls and increasing the risk of data leakage. Additionally, malicious or unintentional misuse of cloud APIs can lead to service disruptions or unauthorized data access [17].

Section IV: Attack Tree

In order to facilitate a clearer understanding of the threats, vulnerabilities and attack techniques described above in Section III, an attack tree model has been developed. In fact, this tree gives a visual representation of the various paths through which cloud based system can be compromised. The attack tree may not cover all possible threat scenarios, but it does summarise the most significant attacks against the most important STEIDE (i.e., Security, Trust, Efficiency, Integrity, Data Protection, and End-user Privacy) principles within cloud environments. An overview of this attack tree is shown in the following section (Page 6).

Conclusion

In today's digital ecosystem, the tech industry heavily relies on web-based technologies, most of which are hosted in cloud environments due to their flexible scalability, high availability, and cost-effectiveness. However, this convenience comes with increased exposure to various security threats and attack surfaces. It becomes imperative to regularly assess potential vulnerabilities and adopt proactive measures to safeguard cloud infrastructure.
This study has explored a broad range of attack vectors and threat models that adversaries may use to compromise cloud-based systems. Special emphasis was placed on the STRIDE framework which serves as a structured method for classifying and understanding these risks.
Additionally, this report introduced the Attack Tree methodology—a powerful visualization tool used to model, analyze, and evaluate possible attack paths within a cloud environment. By mapping out the interrelated threats and vulnerabilities, the attack tree provides a comprehensive security evaluation strategy that aids in identifying critical weaknesses and prioritizing defense mechanisms.
Ultimately, this paper reinforces the importance of continuous threat modeling and secure architecture design in cloud computing. Through the combination of theoretical frameworks like STRIDE and practical tools like attack trees, organizations can enhance their cloud resilience, improve incident response readiness, and reduce their overall security risk.

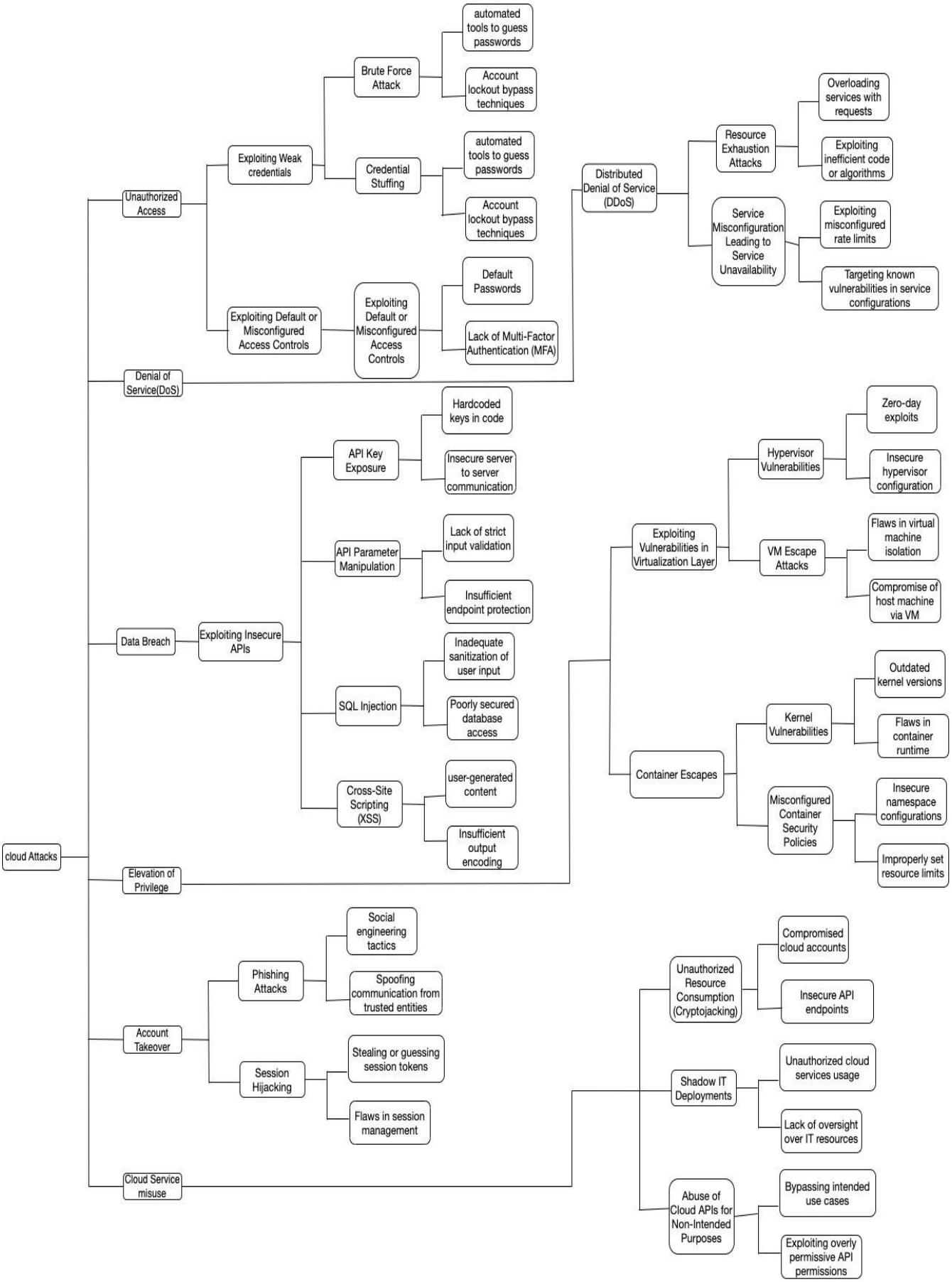

Figure 4: Attack Tree

Use of Generative AI in This Project

To support the research and writing process of this INSE6150 project on cloud security, I used **ChatGPT (OpenAI)** as an educational tool. My use of ChatGPT was limited to tasks that helped me better understand core technical concepts such as STRIDE modeling, attack trees, and various real-world cloud-based threats including brute force, SQL injection, and privilege escalation. I also used the tool to clarify the differences between types of cloud services (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid) through simplified explanations and breakdowns.

Additionally, ChatGPT assisted in:

- **Reformatting and rephrasing my reference list** to ensure originality and reduce Turnitin similarity matches, without altering source accuracy.
- **Proofreading and restructuring parts of the paper** to improve clarity, flow, and academic tone.
- **Creating visual aids** such as redesigned versions of cloud architecture and threat model diagrams to improve presentation.

All critical thinking, analysis, and synthesis of ideas were done independently to demonstrate a clear understanding of the topic. The tool was used to complement, not replace, my own effort.

Related Project Transcripts: https://chatgpt.com/share/68083014-0110-8002-add9-2cb30517b1f4

References

1. *J. Lee, "An Overview of Cloud Computing Concepts," Int. J. Networked & Distributed Comput., vol. 1, no. 1, pp. 2–8, Nov. 2012.*

2. *G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Transforming IT Through Cloud-Based Services," IEEE IT Professional, vol. 11, no. 2, pp. 10–17, Mar.–Apr. 2009.*

3. *Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: Current Landscape and Open Challenges," J. Internet Services and Applications, vol. 1, pp. 7–18, 2010. DOI: 10.1007/s13174-010-0007-6.*

4. *A Singh, "Comprehensive Review of Cloud Security Challenges," J. Netw. & Comput. Appl., vol. 79, pp. 88–201, Oct. 2017. DOI: 10.1016/j.jnca.2016.11.027.*

5. *Google Cloud, "Defining Cloud Security: Concepts and Controls." Accessed April 2024. [Online]. Available: https://cloud.google.com/learn/what-is-cloud-security*

6. *Kaspersky Security Center, "Understanding Cloud Security Principles." Accessed April 2024. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security*

7. *M. Kaur and A. Kaimal, "Resolving Data Breach Risks in Cloud Environments," in Proc. Int. Conf. Comp. Comm. & Informatics (ICCCI), Coimbatore, 2023, pp. 1–6. DOI: 10.1109/ICCCI56745.2023.10128329.*

8. *A. Sharma et al., "A Review of Threat Detection Using ML in Cloud Security," Information, vol. 2, no. 3, 2021. Available: https://www.mdpi.com/2624-800X/2/3/27*

9. *O. Mejri, D. Yang, and I. Doh, "Log-Based Proactive Mitigation of Cloud Security Risks," in Proc. Int. Conf. Adv. Comm. Tech., PyeongChang, 2021, pp. 392–397. DOI:*

10.23919/ICACT51234.2021.9370392.

10. *L. Bhajantri and T. Mujawar, "Cloud Computing Security: Issues and Solutions," in I-SMAC Conf., Palladam, 2019, pp. 376–380. DOI: 10.1109/I-SMAC47947.2019.9032545.*

11. *S. Sanger and R. Johari, "Security Concerns in Modern Cloud Ecosystems," in MECON Conf., Noida, 2022, pp. 490–493. DOI: 10.1109/MECON53876.2022.9751959.*

12. *Joshi et al., "Enhanced Privacy in Cloud Data Security Systems," in Proc. ICFIRTP Conf., Uttarakhand, 2022, pp. 230–233. DOI: 10.1109/ICFIRTP56122.2022.10063186.*

13. *Zimba, H. Chen, and Z. Wang, "Security Analysis of Client-Side Synchronization Attacks," in IEEE ICCC, Chengdu, 2016, pp. 2702–2706. DOI: 10.1109/CompComm.2016.7925189.*

14. *Patil et al., "Adaptive Mitigation of DDoS and Injection Attacks in Cloud Systems," in ICICIC Conf., Indore, 2017, pp. 1–7. DOI: 10.1109/ICOMICON.2017.8279028.*

15. *S. B. Mallisetty et al., "Current Cloud Security Concerns: A Review," in IDCIoT Conf., Bengaluru, 2023, pp. 798–804. DOI: 10.1109/IDCIoT56793.2023.10053520.*

16. *W. de Souza and A. Tomlinson, "Threats in Hypervisor-Free Cloud Architectures," in WorldCIS Conf., London, 2013, pp. 128–133. DOI: 10.1109/WorldCIS.2013.6751032.*

17. *L. Tang, L. Ouyang, and W.-T. Tsai, "Multi-Factor Authentication Strategies for API Security in the Cloud," in FSKD Conf., Zhangjiajie, 2015, pp. 2163–2168. DOI: 10.1109/FSKD.2015.7382287.*

18. *L. H. Pramono and Y. K. Y. Javista, "Securing RESTful APIs Using Firebase in Cloud Apps," in ISRITI Conf., Yogyakarta, 2021, pp. 1–6. DOI: 10.1109/ISRITI54043.2021.9702776.*

Appendix:

Project Attack Tree in Draw.io:

https://drive.google.com/drive/u/0/folders/1-JY5guCqYM_CEAgLvzk7r3EMFcvmq