SoK: Cloud Security Evaluation

Md.Khiruzzaman
Student ID: 40266198

Tonmoy Roy
Student ID: 40271831

Objective

In Today's world, every server is operated from Cloud. Over the last few years, it has witnessed a drastically increase in Usage. As the usage of this service is increasing, the security risk is also increasing with it. This project aims to explore several aspects of Cloud Security. We emphasis on the risk, threat and Vulnerabilities of cloud computing that could be the obstacle for the increasing adoption of cloud computing.

Section I, we focus on the very basics of cloud computing, how they work, the evolution of cloud computing in the tech industry and why the tech industry is moving towards cloud computing. Section II, we explore and gain knowledge on security protocols and mechanisms of cloud computing. In Section III, we start analyzing the threats and vulnerabilities of cloud computing. Section IV illustrates Attack Tree.

Section: I

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

In the past most of the servers were deployed in a physical datacenter and configured as per requirements. But now those scenarios have changed, because of cloud computing. Cloud computing refers to the resources that are available to the user from anywhere, flexible, scalable, secure, and cost efficient.

NIST definition of cloud computing Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[3] There are so many other meanings or definition's available for cloud computing. As per IT user that delivery of computing, storage, and applications over the Internet from centralized data centres. For application developers, it is an Internet-scale software development platform and runtime environment. For infrastructure providers and administrators, it is the massive, distributed data canter infrastructure connected by IP networks [2].
There are 3 types of cloud that are mostly use:

- Public cloud
- Private cloud
- Hybrid cloud

There are 3 types of services that are available in cloud:

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

Cloud will be driven self-service, simplification, standardization, economies of scale, and technology advancement [1].

Are those resources coming from the Sky? (Functioning of cloud computing)

No, the resources of cloud computing are not coming from the sky. Resources are shared from a single or multiple data center which are isolated from each other. In private cloud computing companies host their own resources online, so that their employees can access and operate it from anywhere, also to maintain scalability and security. In public cloud computing companies like AWS (Amazon Web Services), Microsoft Azure and others are hosting their own resources to the customers to give them flexibility, availability, scalability, and security. They have multiple data centers all over the world to give the customers 99.99% availability. Fig.1 shows the overview of how Cloud computing works.

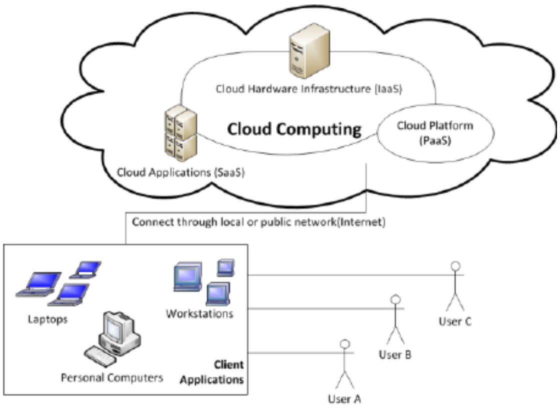
Cloud Hardware Infrastructure (IaaS)
Cloud Computing
Cloud Platform (PaaS)
Cloud Applications (SaaS)
Connect through local or public network(Internet)
Laptops
Workstations
Personal Computers
Client Applications
User C
User B
User A

Figure 1Architecture of Cloud Computing

Why is Tech Industry Moving towards cloud computing?

In the past physical servers were needed to maintain a server and, in that server, only one application was deployed. Then things changed and virtual machines or VM's were introduced, and applications started sharing the same resources within a single server. Still, in distributed computing environments, up to 85 percent of computing capacity sits idle. 66 percent of every dollar on IT is spent on maintaining current IT infrastructures versus adding new capabilities [1] but the revolution in the IT industry started with the introduction of cloud computing. The most important part which attracted the IT industry is there is no upfront cost to use these resources and it was and is helping lot of startup companies to run their applications. Fig.2 shows the Evolution of technology leading to Cloud Computing.

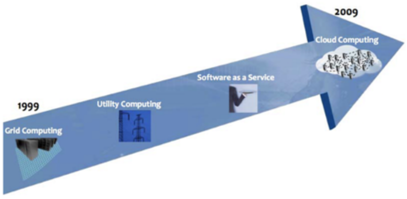

Figure 2 Evaluation of Cloud Computing

Section II: Navigating Cloud Security Essentials

What is Cloud security?

Cloud is built upon two parts among them one is front end or client side another one is backend which is physical resources. Frontend and Backends can also be segmented into

Various parts but cloud security refers to combination of security where it secures the end-user starting from the host [4]. The primary focus of cloud security is on integrating policies, procedures, and technological tools to guarantee data security, facilitate regulatory compliance, and give users and devices control over privacy, access, and authentication [5].

What are the critical areas that need to be secured for cloud environments?

Various sectors need to be secure for the cloud to be secure. The full scope of cloud security is designed to protect the following:

Physical networks: routers, electrical power, cabling, climate controls, etc.

Data storage: hard drives, etc.

Data servers: core network computing hardware and software

Computer virtualization frameworks: virtual machine software, host machines, and guest machines

Operating systems (OS): software that houses.

Middleware: application programming interface (API) management, Runtime environments: execution and upkeep of a running program

Data: all the information stored, modified, and accessed

Applications: traditional software services (email, tax software, productivity suites, etc.)

End-user hardware: computers, mobile devices, Internet of Things (IoT) devices, etc. [6]

In the digital skies where clouds reside, is there any principle guiding stars to secure their wide embrace?

Yes, there are lot of principles for securing the cloud environment. But it maintains the 6 principles of stride.

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- No Repudiation

Section III: Cloud attack surface

Unauthorized Access

Unauthorized access to systems, data, or resources poses significant risks to information security. Such access is primarily enabled by vulnerabilities in the authentication and authorization processes.

Exploiting Weak Credentials

a. Brute Force Attack: This method involves attempting every password combination until the correct one is found. Modern brute force attacks use sophisticated algorithms to optimize password-guessing processes, bypassing even complex and lengthy passwords under certain conditions. Techniques like masking and rule-based attacks refine the guessing strategies, increasing their efficacy [14].

b. Credential Stuffing: Using previously breached username and password pairs, attackers attempt to log in to various websites. This attack relies on the tendency of users to reuse passwords across multiple sites. It is often automated, making it possible to test thousands of credentials within minutes [7].

c. Exploiting Default or Misconfigured Access Controls: Many systems are installed with default credentials which are easily discoverable and often not changed by users. Additionally, the absence of Multi-Factor Authentication (MFA) means that compromising one factor (e.g., password) provides full access, simplifying unauthorized entry [15].

Data Breach

Data breaches can lead to significant financial and reputational damage. They are often the result of exploiting weaknesses in data handling and storage mechanisms.

Exploiting Insecure APIs

a. API Key Exposure: Developers might embed API keys directly within application code, which is then exposed in public repositories or client-side code. Insecure communication between servers can also lead to interception of these keys by attackers [17].

b. API Parameter Manipulation: By manipulating API parameters, attackers can alter the behavior of the API to access unauthorized data or perform unauthorized actions. This often exploits weak input validation to alter SQL queries, retrieve data, or bypass security measures [18].

c. SQL Injection: Attackers can execute arbitrary SQL code on a database server behind a web application by including malicious SQL in a query. This can lead to unauthorized viewing or manipulation of database content [7] [8].

d. Cross-Site Scripting (XSS): XSS attacks occur when attackers inject malicious scripts into content that other users see. Without proper validation and escaping user input, websites can inadvertently execute harmful scripts [11].

Denial of Service (DoS)

Denial of Service attacks incapacitate networks or systems, denying service to legitimate users.

a. Distributed Denial of Service (DDoS): This involves overwhelming the target with traffic from multiple sources, potentially thousands, making it difficult to stop the attack simply by blocking only one source [8][14].

b. Service Misconfiguration: Poorly configured network appliances or application settings can be exploited to amplify DoS attacks. For instance, not setting rate limits on APIs can allow attackers to send innumerable requests without restraint [9][10][15].

Elevation of Privilege

Elevation of Privilege occurs when a user with limited privileges acquires higher-level permissions due to security flaws.

a. Hypervisor Vulnerabilities: These include zero-day vulnerabilities, which are previously unknown flaws that software or hardware vendors have not had time to fix. Attackers exploit these vulnerabilities to perform actions with more privileges than they are entitled to [16].

b. Container and VM Escapes: These attacks exploit security weaknesses in virtualization software and container management systems to escape from a contained environment to the host system, gaining broader access [11].

Account Takeover

This involves gaining control over one or more user accounts, which can lead to data theft and unauthorized transactions.

a. Phishing and Session Hijacking: Phishing employs deceitful tactics to trick users into entering their credentials into fake websites. Session hijacking exploits weak session management to steal authenticated sessions [9][13].

b. OAuth and OpenID Connect Vulnerabilities: These often involve redirecting users to malicious websites during the authentication process or exploiting weak implementations that do not securely validate authentication tokens [13].

Cloud Service Misuse

The adoption of cloud services has introduced unique security challenges, particularly in managing access and monitoring the use of resources.

a. Unauthorized Resource Consumption: Also known as crypto jacking, this involves using someone else's cloud resources to mine cryptocurrency without their consent, often leading to performance degradation and increased costs [12].

b. Shadow IT and API Abuse: Shadow IT involves using unauthorized cloud services without explicit approval from IT departments, which can lead to data leaks and compliance issues. API abuse involves exploiting cloud-based APIs in ways that are inconsistent with their intended use, potentially leading to data exposure or service disruption [17].

Section IV: Attack Tree

Based on the attacks, threats and vulnerabilities discussed in section III, we developed an attack tree. This attack tree is not exhaustive but includes most major threats and attacks on the STEIDE properties of the cloud. The complete attack tree is displayed on the next page (page 6).

Conclusion

The tech industry is mostly based on web technologies, which uses cloud technology for hosting webserver. Besides the scalability and availability of cloud computing, it is the surface for different attacks and threats, which urges to evaluate those security vulnerabilities and take initiative to mitigate them. This report looked at some of the attack and threats which could be used to compromise the cloud technology. It also focuses on the STRIDE properties while exploring those attacks and threats. This project showcases understanding of Cloud computing and different attacks and the security evaluation methodology: Attack Tree.

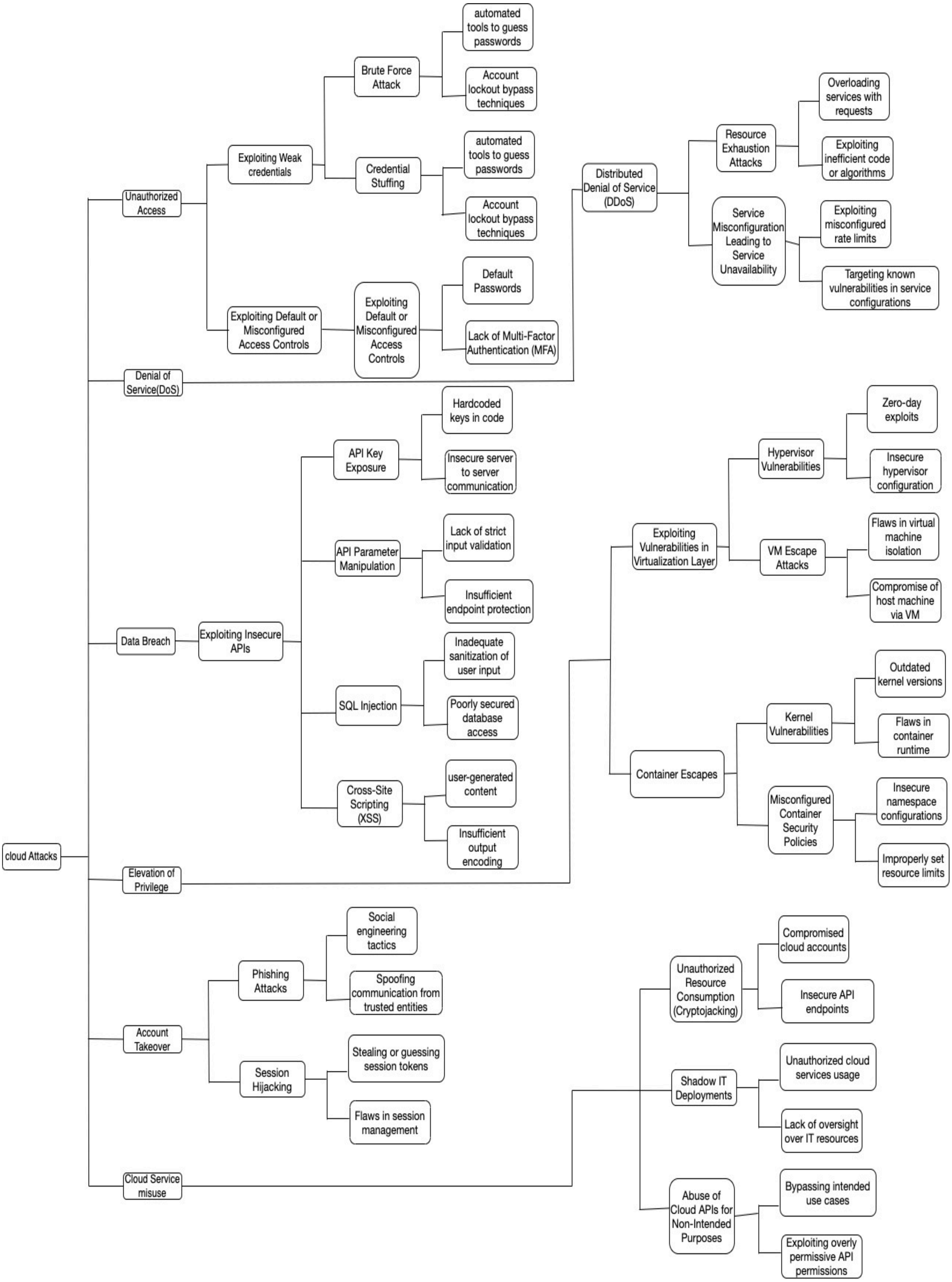
cloud Attacks
Unauthorized Access
Exploiting Weak credentials
Brute Force Attack
automated tools to guess passwords
Account lockout bypass techniques
Credential Stuffing
automated tools to guess passwords
Account lockout bypass techniques
Exploiting Default or Misconfigured Access Controls
Exploiting Default or Misconfigured Access Controls
Default Passwords
Lack of Multi-Factor Authentication (MFA)
Denial of Service(DoS)
Distributed Denial of Service (DDoS)
Resource Exhaustion Attacks
Overloading services with requests
Exploiting inefficient code or algorithms
Service Misconfiguration Leading to Service Unavailability
Exploiting misconfigured rate limits
Targeting known vulnerabilities in service configurations
Data Breach
Exploiting Insecure APIs
API Key Exposure
Hardcoded keys in code
Insecure server to server communication
API Parameter Manipulation
Lack of strict input validation
Insufficient endpoint protection
SQL Injection
Inadequate sanitization of user input
Poorly secured database access
Cross-Site Scripting (XSS)
user-generated content
Insufficient output encoding
Elevation of Privilege
Exploiting Vulnerabilities in Virtualization Layer
Hypervisor Vulnerabilities
Zero-day exploits
Insecure hypervisor configuration
VM Escape Attacks
Flaws in virtual machine isolation
Compromise of host machine via VM
Container Escapes
Kernel Vulnerabilities
Outdated kernel versions
Flaws in container runtime
Misconfigured Container Security Policies
Insecure namespace configurations
Improperly set resource limits
Account Takeover
Phishing Attacks
Social engineering tactics
Spoofing communication from trusted entities
Session Hijacking
Stealing or guessing session tokens
Flaws in session management
Cloud Service misuse
Unauthorized Resource Consumption (Cryptojacking)
Compromised cloud accounts
Insecure API endpoints
Shadow IT Deployments
Unauthorized cloud services usage
Lack of oversight over IT resources
Abuse of Cloud APIs for Non-Intended Purposes
Bypassing intended use cases
Exploiting overly permissive API permissions

Figure 3 Attack Tree

References

1. J. Lee, "A View of Cloud Computing," *International Journal of Networked and Distributed Computing*, vol. 1, no. 1, pp. 2-8, Nov. 19, 2012.
2. G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT as a Service," *IT Pro*, vol. 11, no. 2, Mar./Apr. 2009.
3. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *J Internet Serv Appl*, vol. 1, pp. 7–18, 2010. DOI: 10.1007/s13174-010-0007-6.
4. A. Singh, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88-201, Oct. 2017. DOI: 10.1016/j.jnca.2016.11.027.
5. Google Cloud. (n.d.). "What is Cloud Security?" Retrieved from https://cloud.google.com/learn/what-is-cloud-security.
6. Kaspersky. (n.d.). "What is Cloud Security?" Retrieved from https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security.
7. M. Kaur and A. B. Kaimal, "Analysis of Cloud Computing Security Challenges and Threats for Resolving Data Breach Issues," *2023 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2023, pp. 1-6, doi: 10.1109/ICCCI56745.2023.10128329.
8. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review – https://www.mdpi.com/2624-800X/2/3/27
9. O. Mejri, D. Yang and I. Doh, "Cloud Security Issues and Log-based Proactive Strategy," *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), 2021, pp. 392-397, doi: 10.23919/ICACT51234.2021.9370392.
10. L. B. Bhajantri and T. Mujawar, "A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures," *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2019, pp. 376-380, doi: 10.1109/I-SMAC47947.2019.9032545.
11. A. K. S. Sanger and R. Johari, "Survey of Security Issues in Cloud," *2022 International Mobile and Embedded Technology Conference (MECON)*, Noida, India, 2022, pp. 490-493, doi: 10.1109/MECON53876.2022.9751959.
12. A. Joshi, A. Raturi, S. Kumar, A. Dumka and D. P. Singh, "Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks," *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)*, Uttarakhand, India, 2022, pp. 230-233, doi: 10.1109/ICFIRTP56122.2022.10063186.
13. A. Zimba, Chen Hongsong and Wang Zhaoshun, "Attack tree analysis of Man in the Cloud attacks on client device synchronization in cloud computing," *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2016, pp. 2702-2706, doi: 10.1109/CompComm.2016.7925189.
14. A. Patil, A. Laturkar, S. V. Athawale, R. Takale and P. Tathawade, "A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security," *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, Indore, India, 2017, pp. 1-7, doi: 10.1109/ICOMICON.2017.8279028.

15. S. B. Mallisetty, G. A. Tripuramallu, K. Kamada, P. Devineni, S. Kavitha, and A. V. P. Krishna, “A Review on Cloud Security and Its Challenges,” *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India, 2023, pp. 798-804, doi: 10.1109/IDCIoT56793.2023.10053520.
16. W. A. R. de Souza and A. Tomlinson, “Understanding threats in a cloud infrastructure with no hypervisor,” *World Congress on Internet Security (WorldCIS-2013)*, London, UK, 2013, pp. 128-133, doi: 10.1109/WorldCIS.2013.6751032.
17. L. Tang, Liubo Ouyang and W. -T. Tsai, “Multi-factor web API security for securing Mobile Cloud,” *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, Zhangjiajie, China, 2015, pp. 2163-2168, doi: 10.1109/FSKD.2015.7382287.
18. L. H. Pramono and Y. K. Yana Javista, “Firebase Authentication Cloud Service for RESTful API Security on Employee Presence System,” *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Yogyakarta, Indonesia, 2021, pp. 1-6, doi: 10.1109/ISRITI54043.2021.9702776.

Appendix

GitHub Repository: https://github.com/mkovy39/Concordia-INSE6150-Project
Attack Tree in Draw.io:
https://drive.google.com/file/d/1fCdA3rt7Nr26mZErVtVtU7asdngF1JnS/view?usp=sharing