International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V71I6P113

Volume 71 Issue 6, 73-78, June 2023

Original Article

Securing Cloud Infrastructure: Best Practices for Protecting Data and Applications

Anirudh Mustyala

Software Engineer, Texas, USA.

Corresponding Author : Anirudhmusthyala@gmail.com

Received: 06 May 2023 Revised: 07 June 2023 Accepted: 19 June 2023 Published: 30 June 2023

Abstract *- Leveraging the cloud infrastructure allows businesses to access unlimited storage and innovative technology services. However, the prevalent cloud data and application security risks often cause financial losses, damaged reputation, data loss, and other unwanted consequences. This abstract provides an overview of cloud security infrastructure and examines recent cloud breaches. Also, it discusses the top cloud threats facing businesses today and presents best practices for securing cloud applications and data. The identified top cloud threats include misconfigurations, supply chain and third-party risks, multi-cloud sprawl, and granting users excessive permissions. To mitigate these risks, organizations need to adhere to various best practices. These include implementing identity and access management technologies, maintaining a comprehensive cloud security framework, and reducing cloud attack risks. Furthermore, securing cloud data requires effectively managing access privileges, encrypting all cloud data, ensuring compliance with necessary regulations, and conducting frequent security audits. Adopting these best practices enables businesses to enhance cloud security and protect sensitive data from potential breaches and unauthorized access.*

Keywords *- Cloud security, Cloud data security, Cloud data breaches, Cloud security best practices, Cloud application security, Cloud infrastructure security.*

1. Introduction

In today's fast-paced digital landscape, businesses are increasingly adopting cloud computing, with Gartner forecasting that cloud spending will increase by 21.7% in 2023 [1]. However, securing cloud infrastructure is paramount as it protects valuable data and applications vital for modern organizations. Moreover, reliance on cloud-based assets heightens the need for enhanced integrity and availability [2]. Any security compromise can result in severe consequences, such as unauthorized access, data breaches, service disruptions, and reputational damage.

In addition, cloud environments present unique security challenges. For instance, shared resources in cloud infrastructures introduce exploitable vulnerabilities posing severe security risks [3]. Also, the interconnected nature of the cloud expands the attack surface, making it imperative for businesses to implement robust security practices. Additionally, regulatory requirements and compliance frameworks impose legal obligations on organizations. Hence, they must safeguard sensitive cloud data and applications, reinforcing the need for strong cloud security practices.

2. Understanding Cloud Infrastructure Security

Cloud infrastructure security provides numerous benefits, such as reduced initial capital investment, decreased operational costs, heightened visibility throughout the entire cloud environment, round-the-clock availability, and increased reliability [5]. Moreover, a secure cloud environment allows enterprises to easily adapt application and data storage capacities to meet changing needs while ensuring the security of crucial digital assets.

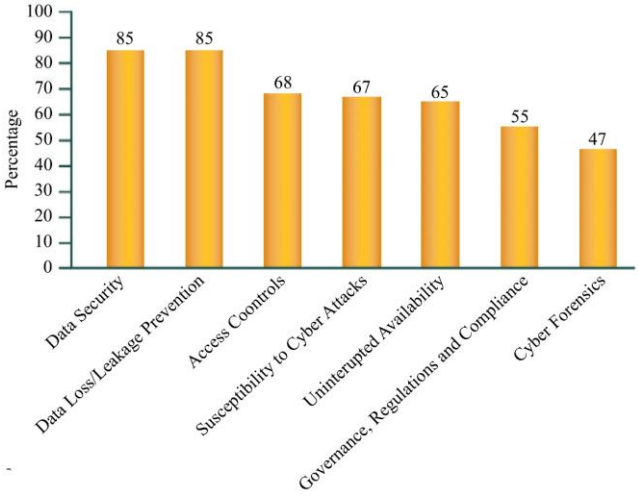

Fig. 1 The leading cloud security concerns [4]

Furthermore, deploying uniform security measures across all cloud environments eliminates the necessity to apply policies to cloud data and applications individually [6]. Specifically, automating crucial security functions like

logging, network surveillance, and threat detection facilitates swift identification and resolution of emerging security challenges. Additionally, comprehensive logs augment visibility and aid organizations in adhering to diverse governance standards, data security regulations, and privacy protocols. More importantly, adopting a robust strategy for securing cloud infrastructure minimizes the cloud environment's attack surface and mitigates security risks to crucial applications and data.

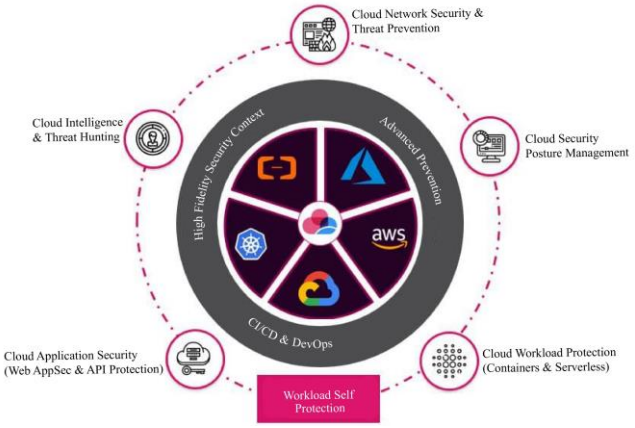

Fig. 2 Cloud Infrastructure Security [7]

3. Recent Cloud Breaches Show That Cloud Security is a Necessity

Recent breaches of different cloud infrastructures emphasize the significance of prioritizing cloud security as a top priority. In particular, these occurrences indicate that enterprises and individuals must acknowledge the indispensability of implementing strong security measures while leveraging cloud services. As businesses increasingly depend on the cloud for storing and managing sensitive data, implementing extensive security protocols is imperative to protect against unauthorized access, data breaches, and potential harm to their reputation and financial well-being [8]. Here are some of the most recent cloud infrastructure attacks and their impacts:

3.1. China's Largest Data Breach in History

Hackers effectively breached a Shanghai police database and acquired the personal information of more than one billion Chinese citizens [9]. The breach is one of the most extensive data disclosures thus far, encompassing individuals' names, contact numbers, government identification numbers, and police records. The perpetrators successfully extracted the data from an Alibaba Cloud database. Subsequent investigation revealed that the database had sufficient security protocols in place. However, the vulnerability stemmed from a publicly accessible management dashboard, which exposed an entry point for hackers to exploit.

3.2. Medibank's Cloud Data Breach Impacts Nine Million Customers

Medibank, a leading health insurance provider in Australia, encountered a significant data breach that impacted at least nine million customers [10]. The breach involved unauthorized entry into the company's cloud-based data network, enabling hackers to access a substantial volume of customer data. Medibank refused to comply despite the attackers' extortion attempt, demanding a ransom. As a result, the hackers released some of the stolen data on the dark web. The compromised data encompassed customer particulars such as names, residential addresses, email addresses, contact information, dates of birth, Medicare numbers, and specific health claims data.

3.3. Kronos Ransomware Attack Impacts Puma Employees

Puma, a global sportswear manufacturer, was among the organizations impacted by a ransomware attack that targeted Kronos, a cloud-based HR management organization [11]. The attack occurred in December 2021. According to Kronos, the hackers gained unauthorized entry into the Kronos Private Cloud (KPC) environment. Before deploying ransomware, they extracted data, which included information belonging to more than 6,000 Puma employees [12]. The stolen files included Social Security Numbers. However, Puma clarified that the attack was limited to Kronos' Private Cloud and that none of its internal network systems was compromised.

4. Top Cloud Threats Facing Businesses Today

4.1. Cloud Misconfigurations

The primary cause of most cloud security breaches is misconfiguration. These include inadvertently disclosing cloud interfaces and infrastructure to the internet. Cloud misconfigurations provide attackers with vulnerabilities that they can exploit to infiltrate the cloud environment [13]. Moreover, insiders with malicious intents can intentionally orchestrate misconfigurations, and their activities might remain unnoticed due to the absence of comprehensive cloud security tools.

Threat actors continuously and actively attempt to exploit misconfigured cloud systems. An example from 2022 is attackers specifically targeting publicly accessible misconfigured Elasticsearch cloud buckets to exfiltrate unprotected data and substitute it with ransom notes [15]. However, even renowned cloud providers like Microsoft [16] and Amazon [17] have encountered security scares due to misconfigurations that resulted in data leaks within their respective cloud environments.

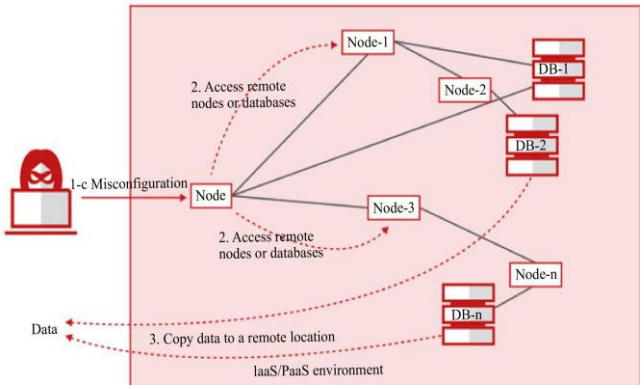

Fig. 3 Cloud misconfiguration security threats [14]

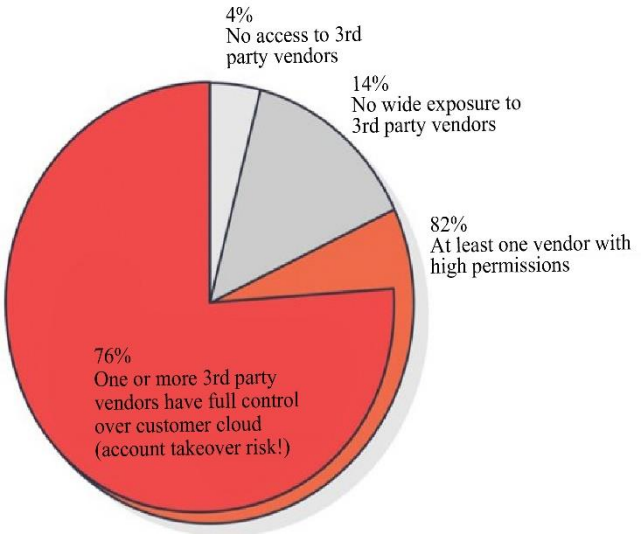

Fig. 4 How much cloud data is exposed to third-party risk? [20]

4.2. Supply Chain and Third-Party Risks

In December 2022, attackers successfully infiltrated a cloud server hosted on Amazon Web Services (AWS) [18]. Tequivity, a third-party provider responsible for delivering asset management and tracking services to the renowned ride-sharing company Uber, uses the cloud server. As a result, the breach compromised sensitive data linked to approximately 77,000 Uber employees and other company-related information [19]. The incident is a clear reminder of the inherent dangers associated with third-party software and the vulnerabilities that can arise within supply chains, particularly within cloud environments.

While it is a commonplace for third-party entities to access data or applications within the cloud, it introduces a singular point of failure that malicious actors can exploit [21]. "If we're using a third party that is legitimate and we connect it to our application because it's a service we're using, and that service gets exploited, it might not get detected as an abnormal or malicious activity because the vulnerability lives outside our security perimeter," notes Shira Shamban, Solvo's CEO [22].

4.3. Multi-Cloud Sprawl

A notable challenge in most cloud deployments is the lack of a unified, centralized cloud infrastructure. According to statistics, the adoption of multi-cloud strategies differs, with some sources indicating that approximately 92% of companies have embraced multi-cloud strategies [23]. In contrast, others suggest that 64% of organizations utilize at least two cloud models [24].

Irrespective of those figures, incorporating multiple clouds introduces security complexities commonly called "multi-cloud sprawl." Security challenges emerge from the continual expansion of data and its dispersion across dynamic locations within these diverse clouds [25]. Consequently, tracking and securing data becomes increasingly arduous due to its scattered nature.

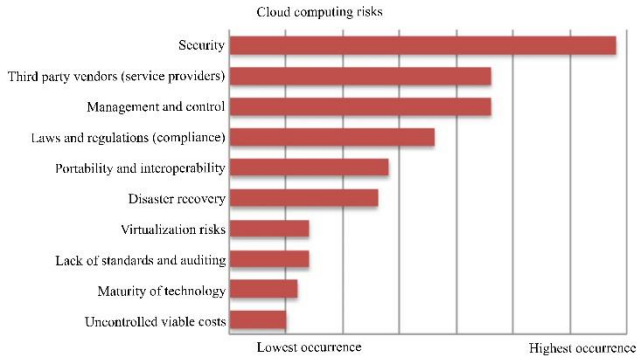

Fig. 5 The leading cloud security risks and challenges [28]

4.4. Granting Users Excessive Permissions

The cloud offers IT administrators high flexibility as they can control service access based on users' roles within the organization. Unlike physical environments, the security of cloud workloads relies on permissions assigned to users and devices within the cloud environment. In theory, this approach should enhance security by limiting individuals' access to applications, thus reducing the potential impact of compromised credentials in the hands of threat actors [26].

However, cloud environments frequently encounter a significant over-permissioning threat in practice. Research conducted by Palo Alto Networks' Unit 42 revealed that approximately 99% of cloud users, resources, services, and roles possess excessive permissions that remain unused [27]. Overpermissioning poses a security risk.

5. Best Practices for Securing Cloud Applications

5.1. Implement Identity and Access Management Technologies

Deploying identity access management (IAM) is crucial to securing cloud applications. In particular, integrate IAM into the broader organizational security practices to establish a comprehensive security approach. IAM verifies user identities, granting access to appropriate data and application functions and ensuring a robust security framework. Therefore, organizations should employ IAM technology to manage user identities and access permissions effectively.

IAM facilitates initiating, capturing, storing, and administrating user identities and associated access privileges. Additionally, it ensures that access rights align with established policies set by security administrators and developers. Moreover, IAM guarantees proper authentication, authorization, and auditing for individuals and services interacting with cloud applications. In other words, IAM can enable organizations to fortify their overall security posture and safeguard their cloud applications.

5.2. Maintain a Comprehensive Cloud Security Framework

Establish robust and consistent policies to ensure the continuous security of cloud-based assets. The policies must

clearly outline the authorized users for each application and specify the methods for verifying access. Furthermore, integrating advanced security measures like multi-factor authentication IAM strengthens the security of cloud applications.

Developing a comprehensive security framework encompassing all cybersecurity aspects is particularly important. Such a framework should consist of network, infrastructure, endpoint, and cloud security controls. Furthermore, the cloud security architecture should address critical elements of the cloud infrastructure. These include data security, continuous monitoring, full visibility, threat detection, cloud governance, and regulatory compliance.

5.3. Reduce Cloud Attack Risks

Every cloud-based application expands the attack surface, thus increasing the potential entry points for attackers. Fortunately, you can mitigate these risks through two primary approaches. First, maintain an updated inventory of all cloud assets, workloads, and applications. An updated inventory enhances visibility and provides a comprehensive understanding of the cloud environment. You can effectively monitor, manage, and secure their cloud assets with a clear inventory. Secondly, limit the attack surface by regularly reviewing and assessing the necessity of each application or workload within the cloud environment. Remove any applications or workloads that are not essential for business operations.

6. Best Practices for Securing Cloud Data

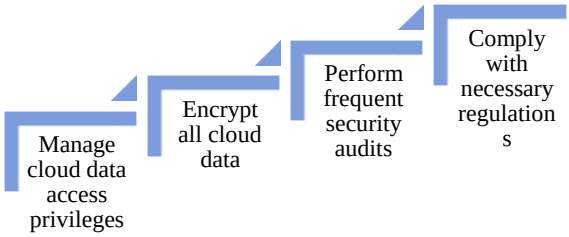

Fig. 6 Best practices for protecting cloud data

6.1. Effectively Manage Access Privilege to Cloud Data

It is vital to manage user access privileges to strengthen cloud data security effectively. Providing excessive and unnecessary access to data increases the risk of potential compromise and unauthorized access. Therefore, regularly review and revoke all cloud users and devices' unused or excessive user privileges. For instance, adhering to the principle of least privilege ensures that you grant users access only to the specific data and systems required for their job roles.

Additionally, establishing well-defined procedures for employee onboarding and offboarding, including creating and terminating accounts and managing associated access privileges, protects cloud data from unauthorized access. It also ensures controlled access permissions that align with employees' roles and responsibilities, thereby reducing the risk of data compromise.

6.2. Encrypt All Cloud Data

Encryption plays a critical role in upholding cloud data security. Encrypting data at rest and in transit protects it from breaches, unauthorized access, and misuse. Applying encryption measures for data at rest ensures that even if the data is compromised, it remains unintelligible to unauthorized parties.

Similarly, encrypting data during transit is equally vital, as it is more susceptible to attacks. Encryption preserves data integrity and confidentiality even if attackers manage to intercept it as it transits from the cloud to a device and vice versa.

Many cloud computing providers offer encryption and key management services; third-party cloud and software companies provide encryption options. Hence, choose an encryption solution that seamlessly integrates with existing workflows, minimizing the need for end users to comply with encryption policies established by the organization.

6.3. Ensure Compliance with Necessary Regulations

Organizations operating in highly regulated industries like healthcare and financial services must comply with numerous regulations. Most companies also collect and process personally identifiable information (PII) and are subject to stringent data regulations created to ensure customer privacy and data security. Moreover, businesses operating in specific geographic locations or storing data within certain regions may encounter additional compliance requirements imposed by state governments.

When considering adopting a new cloud computing service, organizations must thoroughly review their specific compliance requirements. This entails assessing whether a potential service provider can meet the required data security standards and regulatory obligations. Compliance should be a priority since regulatory bodies hold companies responsible for compliance violations or data breaches, even if the cloud provider is responsible.

6.4. Perform Frequent Security Audits

Irrespective of whether an organization chooses to outsource security functions to an external firm or manage them internally, experts highly recommend conducting penetration tests and vulnerability scans. These practices are essential for evaluating the efficacy of current cloud security measures in protecting data and applications. Also, they pinpoint security flaws and misconfigurations that threaten cloud data security, allowing the organization to mitigate them accordingly.

7. Conclusion

Implementing robust security measures is crucial for safeguarding cloud infrastructure and ensuring the protection of valuable data and applications. Additionally, the ever-evolving nature of cyberattacks requires a proactive and comprehensive approach to security. Securing cloud infrastructure is not a one-time effort but an ongoing

commitment essential for building trust, maintaining compliance, and preserving business continuity.

Security threats in cloud environments can cause large data breaches that damage the organization's reputation. Misconfigurations are a primary cause of breaches, where unintentional or intentional errors expose vulnerabilities for attackers to exploit.

Supply chain and third-party risks emphasize the dangers associated with granting external entities access to cloud systems. Also, multi-cloud deployments introduce complexities in tracking and securing data dispersed across diverse clouds. Furthermore, granting users excessive permissions poses a significant security risk, with unused permissions being prevalent and potentially exploited by malicious actors.

Therefore, countering these threats requires strong and effective cloud security measures. These include strong identity and access management protocols to control user privileges and minimize the risk of unauthorized access. Also, encrypting data at rest and in transit adds a security layer, ensuring the confidentiality and integrity of sensitive information. Moreover, regular monitoring, vulnerability assessments, and penetration testing are vital for proactively identifying and addressing potential vulnerabilities.

Besides, organizations must recognize that securing cloud infrastructure goes beyond technical measures. It requires a comprehensive understanding of regulatory requirements and compliance frameworks relevant to their industry. Aligning security practices with these standards demonstrates a commitment to data protection and meeting legal obligations.

References

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023#:~:text=All%20segments%20of%20the%20cloud,%25%20(see%20Table%201).

[2] Ariel (Eli) Levite, and John Pendleton. Cloud Reassurance Project: Interim Report, 2023. [Online]. Available: https://carnegieendowment.org/publications/89927?utm_source=rss&utm_medium=rss

[3] Shaikh Ashapakh Sattar, "Security Issues in Cloud Services," *International Journal of New Technology and Research*, vol. 2, no. 6, pp. 8-10, 2016. [Publisher Link]

[4] Asif Iqbal et al., "Secure Data in Cloud on the Basis of Sensitivity," *Journal of Applied Environmental and Biological Sciences*," [Google Scholar] [Publisher Link]

[5] Yunusa Simpa Abdulsalam, and Mustapha Hedabou, "Security and Privacy in Cloud Computing: Technical Review," *Future Internet*, vol. 14, no. 1, pp. 1-27, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Omar Ali et al., "Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities," *Government Information Quarterly*, vol. 37, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] What is Cloud Security? [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

[8] Rakesh Kumar, and Rinkaj Goyal, "On Cloud Security Requirements, Threats, Vulnerabilities and Countermeasures: A Survey," *Computer Science Review*, vol. 33, pp. 1-48, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] [Online]. Available: https://blog.leakix.net/2022/07/what-we-know-about-the-china-leak/

[10] Medibank Hackers Announce 'Case Closed' and Dump Huge Data File on Dark Web. [Online]. Available: https://www.theguardian.com/australia-news/2022/dec/01/medibank-hackers-announce-case-closed-and-dump-huge-data-file-on-dark-web

[11] [Online]. Available: https://ago.vermont.gov/wp-content/uploads/2022/02/2022-02-03-PUMA-North-America-Data-Breach-Notice-to-Consumers-ID-269612.pdf

[12] [Online]. Available: https://apps.web.maine.gov/online/aeviewer/ME/40/10394643-6f4e-49ff-884a-9977602932a9.shtml

[13] James Guffey, and Yanyan Li, "Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions," *In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0806-0812, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] [Online]. Available: https://www.helpnetsecurity.com/2019/09/25/cloud-misconfiguration-incidents/

[15] 12K Misconfigured Elasticsearch Buckets Ravaged by Extortionists. [Online]. Available: https://www.darkreading.com/cloud/12k-misconfigured-elasticsearch-buckets-extortionists

[16] Investigation Regarding Misconfigured Microsoft Storage Location. [Online]. Available: https://msrc-blog.microsoft.com/2022/10/19/investigation-regarding-misconfigured-microsoft-storage-location-2/

[17] Zack Whittaker, Amazon Accidentally Exposed an Internal Server Packed with Prime Video Viewing Habits. [Online]. Available: https://techcrunch.com/2022/10/27/amazon-prime-video-server-exposed/

[18] ISBuzz Staff , Tequivity Cloud Server Compromise Leads to Uber Breached, Experts Reacted. [Online]. Available: https://informationsecuritybuzz.com/tequivity-cloud-server-compromise-leads-to-uber-breached-experts-reacted/

[19] [Online]. Available: https://thecyberexpress.com/uber-data-leak-cyber-attack-vendor-teqtivity/

[20] Josh Dreyfuss, How to Protect Your Cloud Environment from Supply Chain Attacks. [Online]. Available: https://www.wiz.io/blog/how-to-protect-your-cloud-environment-from-supply-chain-attacks

[21] Theresa Sobb et al., "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics*, vol. 9, no. 11, 1864. [CrossRef] [Google Scholar] [Publisher Link]

[22] [Online]. Available: https://blog.neterra.cloud/en/%D0%B2%D0%BE%D0%B4%D0%B5%D1%89%D0%B8%D1%82%D0%B5-%D0%B7%D0%B0%D0%BF%D0%BB%D0%B0%D1%85%D0%B8-%D0%B7%D0%B0-%D0%BA%D0%BB%D0%B0%D1%83%D0%B4%D0%B0-%D1%81-%D0%BA%D0%BE%D0%B8%D1%82%D0%BE-%D1%82%D1%80%D1%8F/

[23] [Online]. Available: https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report

[24] [Online]. Available: https://www.sdxcentral.com/articles/news/nutanix-report-64-of-orgs-will-adopt-multi-cloud-within-3-years/2022/01/

[25] Rory Duncan, "A Multi-Cloud World Requires a Multi-Cloud Security Approach," *Computer Fraud & Security*, vol. 2020, no. 5, pp. 11-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Aamir Syed, Keerthana Purushotham, and Ganeshayya Shidaganti, "Cloud Storage Security Risks, Practices and Measures: A Review," *In 2020 IEEE International Conference for Innovation in Technology (INOCON*, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] [Online]. Available: https://www.paloaltonetworks.com/resources/research/unit42-cloud-with-a-chance-of-entropy

[28] Mariana Carroll, Alta van der Merwe, and Paula Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls," *2011 Information Security for South Africa*, pp. 1-9, 2011. [CrossRef] [Google Scholar] [Publisher Link]