International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I11P115

Volume 72 Issue 11, 143-149, November 2024

Original Article

Effective Multi Cloud Security Using AI Technologies

Naresh Kumar Miryala

Meta Platforms – USA.

Corresponding Author : nmiryala@gmail.com

Received: 01 October 2024 Revised: 02 November 2024 Accepted: 22 November 2024 Published: 30 November 2024

Abstract *- In the current dynamic IT landscape, the importance of multi-cloud environments introduces multifaceted challenges in securing organizational data. This abstract navigates the intersection of multi-cloud security and Artificial Intelligence (AI), presenting a succinct yet comprehensive overview of strategies to fortify against evolving cyber threats. Multi-cloud adoption, while enhancing agility, necessitates advanced security measures. This abstract emphasizes the imperative of a sophisticated approach to safeguard data across diverse cloud platforms. Exploring the multi-cloud security landscape, we scrutinize data protection intricacies, identity management nuances, and compliance considerations. This sets the stage for integrating AI solutions to address these challenges effectively.Artificial intelligence, encompassing machine learning and predictive analytics, emerges as a transformative force. We discuss AI's potential to revolutionize threat detection, response mechanisms, and policy enforcement within the complex dynamics of multi-cloud environments. Proactive threat detection and prevention are paramount. AI algorithms play a pivotal role in continuously monitoring and analyzing vast datasets for anomalous behavior, providing resilient defense mechanisms against emerging threats. Ensuring consistent security policies across diverse cloud providers remains a challenge. This abstract explores the role of AI-powered orchestration tools in unifying security measures, streamlining policy enforcement, and simplifying the management of security protocols. In conclusion, this abstract underscores the urgency for organizations to adopt AI-driven strategies, offering a concise yet insightful overview of the critical intersection between multi-cloud security and artificial intelligence. It provides a strategic roadmap for organizations aiming to fortify their security posture in the intricate landscape of multi-cloud environments. The paper begins by delving into the unique security considerations posed by multi-cloud deployments, addressing the intricacies of managing data across disparate platforms while adhering to regulatory requirements.*

Keywords *- Multi-cloud security, Artificial Intelligence(AI), Cyber security, Threat detection, Data protection, Identity management, Compliance, Cloud security, Machine learning, Predictive analytics, Security automation, Resilient security, Threat prevention, Governance, Data encryption, Privacy compliance, Continuous security monitoring, Security protocols, Cloud providers, Security frameworks, Anomalous behavior detection, Security posture, Agility in IT, Resource optimization, Regulatory requirements, Industry standards, Intelligent key management, Access control, Dynamic IT ecosystems, Threat landscape, Security challenges, Complex IT environments, Security strategies, Integration of AI in security, Security measures, Policy enforcement, Streamlining security, Complexity management.*

1. Introduction

In an age where digital transformation is steering organizations towards adopting multi-cloud environments, the convergence of agility and innovation brings forth a unique set of security challenges. As businesses harness the potential of diverse cloud providers to optimize operations and scale infrastructure, a resilient and adaptive security framework becomes paramount. This introduction sets the stage for a focused exploration of the intersection between multi-cloud security and Artificial Intelligence (AI), where traditional security measures meet the transformative capabilities of advanced technologies. The following sections will delve into the intricacies of securing multi-cloud environments, acknowledging the complexities of various cloud platforms' coexistence.

In the ever-changing world of multi-cloud security, traditional security approaches must evolve. Artificial Intelligence (AI) plays a crucial role in strengthening defenses. Whether it is identifying and stopping threats, coordinating security measures, ensuring compliance, or keeping a constant watch, AI is set to transform how organizations protect their digital assets in the vast landscape of multi-cloud setups. This white paper embarks on a journey to unravel the symbiotic relationship between multi-cloud security and AI. Through a strategic lens, we will explore how AI technologies, including machine learning and predictive analytics, not only detect and respond to threats in real-time but also enhance the overall resilience and agility of security measures. As we navigate this exploration, the objective is clear: to provide organizations with a foundational

understanding of the challenges posed by multi-cloud security and illuminate AI's transformative potential in mitigating these challenges. The following chapters will delve into specific areas where AI plays a pivotal role, offering actionable insights and strategic considerations for securing multi-cloud environments in an era of connectivity, complexity, and the relentless pursuit of digital innovation.

2. What is Multi Cloud?

Multi-Cloud means a software app can work on different cloud services (like AWS, Azure, or a private cloud) without needing to change the code. This is great because it lowers costs, makes businesses more flexible, and better prepares them for the future. They can easily switch from one cloud provider to another if they want. Multi-cloud security is the suite of strategies, controls, procedures, and technologies designed to protect a multi-cloud environment's data, applications, and associated infrastructure. In a multi cloud setup, an organization uses multiple cloud services from different cloud providers, which could be a mix of public, private, or hybrid clouds. Multi-cloud security is a comprehensive cloud security solution that protects and prevents enterprise and customer data, assets and applications from advanced security threats and cyberattacks across multiple cloud infrastructures and environments. Multi-cloud security is a way of handling security challenges when a company uses multiple cloud service providers. Instead of relying on just one cloud, they use two or more, each with its services and functions. With multi-cloud security, they put strong measures in place to protect their data, apps, and computer infrastructure in all these different cloud environments. In essence, it encompasses the deployment of security protocols, tools, and strategies tailored to the intricacies of a multi-cloud ecosystem. This includes considerations for data protection, identity management, compliance adherence, and the dynamic nature of threat landscapes across varied cloud providers. As businesses increasingly migrate to the cloud to leverage its benefits, they expose themselves to new security risks.

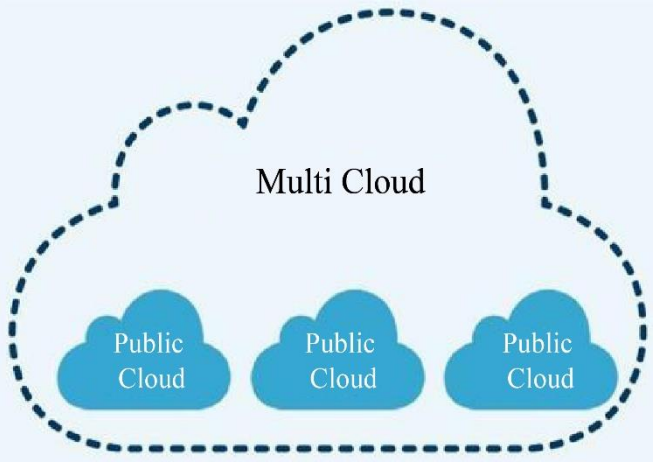

Fig. 1 Multi Cloud Example

These risks can be magnified in a multi cloud environment due to the increased complexity and the need to secure data across multiple platforms. The evolution of multi cloud security has been driven by the growing adoption of cloud services and the increasing sophistication of cyber threats. Initially, cloud security focused on securing a single cloud environment. However, as organizations started to use multiple cloud services, the need for a more comprehensive approach to security became apparent.

2.1. Why is it Important?

Multicloud security is most important in the digital landscape due to the transformative shift toward utilizing multiple cloud service providers. This strategic adoption offers organizations unparalleled flexibility, scalability, and operational efficiency.

However, with these benefits come intricate security challenges requiring a dedicated focus on multicloud security. Firstly, the distributed nature of data and applications across various cloud environments increases the attack surface, amplifying the risk of unauthorized access and data breaches. Secondly, diverse cloud providers often have distinct security protocols and interfaces, demanding a cohesive security strategy to ensure consistent protection. Compliance with regulatory standards further underscores the significance of multicloud security, ensuring that organizations meet legal requirements while safeguarding sensitive information. Ultimately, the importance of multicloud security lies in its role as a proactive defense against a dynamic threat landscape, enabling organizations to harness the benefits of multicloud architectures while maintaining the integrity, confidentiality, and availability of their digital assets.

2.1.1. Increased reliability

Multicloud security helps ensure that your business assets, like data and important applications, stay safe. It adds an extra layer of protection, allowing only authorized users to access applications. This helps prevent any unauthorized access and keeps sensitive information from leaking.

2.1.2. Constant security

Your business benefits from continuous monitoring for cyberattacks and potential risks in a more secure cloud setup. You also get timely reminders about important security updates. This constant watch helps protect your digital assets and ensures that your systems are up-to-date against potential threats.

2.1.3. Reduced Costs

Cyberattacks can cause serious harm to your business, leading to expensive repairs and recovery efforts. By securing your multicloud setup, you are taking steps better to protect your business from the costly consequences of cyberthreats. This helps minimize the potential damage and financial impact of such attacks.

Fig.2 Multi Cloud Data Security

2.1.4. Centralized Visibility

A multicloud security solution makes it easy for your business to handle the security of all your cloud setups from one place. With this, you can check the status of your applications, evaluate any risks related to data or application exposure, and control who has access to your systems. It is like having a central control center for managing the security of your various cloud environments.

3. Role of AI in Multi Cloud Security

The role of AI in Multi cloud security is as follows:

3.1. Evolution of Multi Cloud Security with AI:

The landscape of multi-cloud security is undergoing a transformative evolution, and at its nucleus lies the integration of Artificial Intelligence (AI) technologies. As organizations navigate the complexities of securing data and applications across multiple cloud environments, AI emerges as a powerful catalyst, promising to enhance traditional security measures and to revolutionize how threats are detected, responses are formulated, and overall security postures are maintained.

Fig. 3 AI in multi cloud security

3.2. Threat Protection

One of the primary roles of AI in multi-cloud security is witnessed in threat detection. Cyber threats are always changing, so it is important to be proactive. AI, using advanced machine learning algorithms, helps organizations spot unusual activities and potential security breaches as they happen in real-time. By continuously analyzing vast datasets and identifying patterns indicative of malicious activities, AI empowers security teams to stay ahead of emerging threats.

3.3. Proactive Defense Mechanisms

AI's role extends beyond mere threat detection; it actively contributes to establishing proactive defense mechanisms. Machine learning models, trained on historical data and evolving threat landscapes, equip security systems to predict and prevent potential security incidents. This capability enables organizations to address vulnerabilities before they are exploited, fostering a resilient security posture in the dynamic multi-cloud environment.

3.4. Unified Security Orchestration and Automation

AI's impact is prominently felt in the realm of security orchestration and automation. In a multi-cloud ecosystem where maintaining consistent security policies across diverse providers is paramount, AI-powered orchestration tools streamline and automate security measures. This ensures policy adherence and simplifies the complex task of managing disparate security protocols across varied cloud infrastructures.

3.5. Identity and Access Management(IAM)

Identity and Access Management (IAM) are really important for keeping things secure in a multi-cloud setup. AI brings its abilities to make IAM frameworks even better and more effective. Through adaptive authentication and continuous monitoring, AI-driven IAM systems analyze user behavior patterns to detect anomalies, fortifying access controls and ensuring a secure user experience across different cloud environments.

Fig. 4 Multi Cloud IAM Security

3.6. Data Protection and Encryption

In data protection, AI plays a pivotal role in strengthening encryption methods. AI-driven encryption is like a smart way of keeping information safe, whether sitting somewhere or moving from one place to another. It ensures that sensitive data stays confidential and intact, protecting it from unauthorized access or tampering. Additionally, AI assists in developing intelligent key management systems, contributing to robust data protection measures within the multi-cloud architecture.

3.7. Continuous Monitoring and Predictive Analytics

Continuous security monitoring, powered by AI, offers organizations a real-time understanding of network traffic, user activities, and system behaviors across the multi-cloud landscape. Through predictive analytics, AI facilitates proactive identification of potential security threats, enabling timely responses and reducing the impact of security incidents.

3.8. Adaptive Incident Response

In a security incident, AI enhances the incident response mechanism. By automating the analysis of incident data, correlating information from different cloud sources, and facilitating rapid decision-making, AI ensures a swift and adaptive response to security breaches. This integration accelerates response times and minimizes the impact on the organization's security posture.

3.9. Threat Intelligence

Harnessing AI for threat intelligence is a strategic imperative in the multi-cloud security paradigm. AI technologies aggregate and analyze vast datasets from diverse sources, enabling organizations to stay ahead of emerging threats, understand evolving attack vectors, and adapt their security strategies accordingly. AI-driven threat intelligence positions organizations to proactively address emerging risks in the ever-evolving multi-cloud landscape.

3.10. Future-Proofing Multi-Cloud Security

Looking ahead, the role of AI in multi-cloud security is synonymous with future-proofing. As AI technologies evolve, organizations can seamlessly integrate new tools and algorithms into their security frameworks, ensuring their defenses remain at the forefront of innovation. The fusion of multi-cloud security with AI addresses presents challenges and positions organizations to tackle future uncertainties with agility and resilience.

4. Need for Multi Cloud

Securing a multi-cloud network is critical, given the dynamic and distributed nature of resources across various cloud service providers. Effectively managing security in this environment involves addressing a range of challenges and implementing comprehensive strategies. Here are key considerations for securing a multi-cloud network:

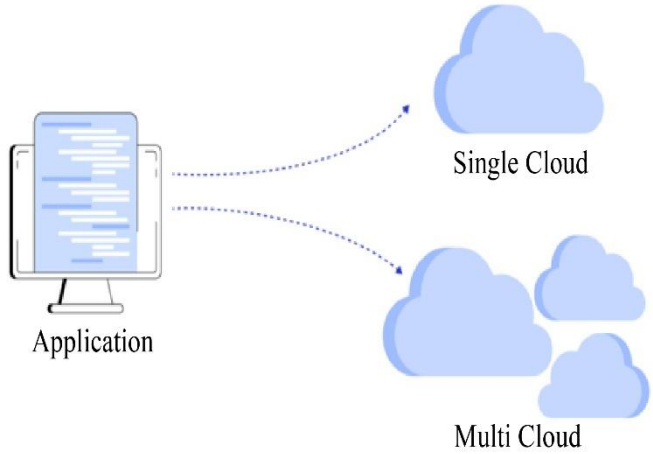

Fig. 5 Multi cloud requirement

4.1. Network Segmentation

Implementing robust network segmentation is foundational. By dividing the network into distinct segments, organizations can contain potential breaches, limiting the lateral movement of threats within the multi-cloud environment.

4.2. Zero Trust Security Model

Embracing a Zero Trust security model is essential. This approach assumes no implicit trust, even within the network. Every user and device, inside or outside the network perimeter, must be authenticated and authorized before access.

4.3. Encryption of Data in Transit and at Rest:

Encrypting data both in transit and at rest is a fundamental security measure. Strong encryption protocols ensure that even if data is intercepted, it remains unreadable to unauthorized entities.

4.4. Secure APIs and Inter-Cloud Communication

Given the interconnected nature of multi-cloud environments, securing APIs and communication between cloud services is critical. Implementing secure API gateways and encryption for inter-cloud communication helps safeguard data integrity.

4.5. Cloud-Native Security Services

Leveraging built-in security services provided by cloud providers enhances protection. Features such as firewalls, Web Application Firewalls (WAF), and security groups specific to each cloud platform contribute to a robust security posture.

4.6. Continuous Monitoring and Logging

Implementing continuous monitoring tools and centralized logging solutions is crucial for detecting and responding to security incidents in real-time. Monitoring network traffic, user activities, and system behavior provides insights into potential threats.

4.7. Threat Detection and Response

Businesses can better spot and deal with changing cyber threats by using smart threat detection solutions that rely on Artificial Intelligence (AI) and machine learning (ML). These technologies allow for quick and automated responses to security issues, helping to minimize potential incidents' impact promptly.

4.8. Regular Security Audits and Assessments

Regular security audits and assessments are essential for identifying vulnerabilities and ensuring compliance with security policies. Regular reviews help organizations avoid potential risks and maintain a resilient security posture.

4.9. Incident Response Planning

Developing and regularly testing an incident response plan is crucial. A well-defined process for responding to security incidents, including communication protocols and remediation steps, minimizes the impact of a security breach.

4.10. Collaboration with Cloud Service Providers

Engaging in collaborative efforts with cloud service providers is vital. Understanding the security features and best practices each provider offers ensures organizations can leverage native security capabilities effectively.

4.11. Compliance Management

Organizations need to follow industry rules and data protection laws. Businesses that operate in different places need to stay updated on the specific requirements in each location and take steps to meet those standards. This helps them ensure they follow the necessary regulations and secure data.

4.12. Regular Updates and Patch Management

Keeping all software, including operating systems and security tools, up to date is crucial. Regularly applying patches and updates helps address known vulnerabilities and enhances the overall security of the multi-cloud network.

5. Implementing Multi-Cloud Security

Securing a multi-cloud environment is intricate, but adherence to best practices can streamline the process:

5.1. Centralized Security Management Platform:

Utilize a single security management platform to monitor everything and manage security across various cloud providers. This centralized approach allows for automated security controls and ensures policies are consistently enforced. It is like having a control center that oversees and manages security across all your cloud services in one place.

5.2. Consistent Security Practices and Policies:

Make sure to apply the same security rules and policies across all your cloud providers. This includes managing identities, controlling network security, protecting web applications and APIs, securing data, following compliance standards, and detecting and responding to threats. Keeping these practices consistent across all your cloud services helps maintain a strong and uniform security approach.

5.3. Comprehensive Protection with Consistent Policies:

Set up complete protection with the same security rules everywhere, keeping things safe in complicated setups, including older and newer applications, various cloud services, and different data centers. This helps ensure a consistent and strong security shield across the complex environment.

6. Advantages of AI in Multi Cloud Security

A multi-cloud AI strategy, leveraging the power of Artificial Intelligence across various cloud service providers, offers a myriad of advantages that enhance flexibility, resilience, and innovation within an organization’s digital infrastructure.

6.1. Redundancy and High Availability

Embracing a multi-cloud AI strategy allows organizations to distribute workloads across cloud platforms. This redundancy ensures high availability and minimizes the risk of downtime, as operations can seamlessly shift between cloud providers in the event of an outage.

6.2. Optimized Performance and Scalability

Leveraging multiple cloud providers enables organizations to select services that best suit their needs. This optimization enhances overall performance and scalability, allowing for dynamic adjustments in computational resources based on demand.

6.3. Cost Optimization

A multi-cloud AI strategy promotes cost efficiency by enabling organizations to choose the most cost-effective services from different providers. This flexibility facilitates strategic cost management, aligning expenses with performance requirements.

6.4. Vendor Diversification and Negotiation Power

Utilizing multiple cloud providers reduces dependency on a single vendor, fostering competition and providing organizations with negotiation leverage. This diversity ensures that organizations are not beholden to a single provider’s pricing models or service offerings.

6.5. Geographic Diversity and Data Residency Compliance

Organizations can strategically distribute data and applications across geographically dispersed cloud regions, ensuring compliance with data residency regulations. This geographic diversity also enhances data resilience and reduces latency for global operations.

6.6. Innovation and Access to Cutting-Edge Services

A multi-cloud approach enables organizations to leverage different cloud providers' unique strengths and specialized

services. This access to cutting-edge AI tools and services fosters innovation and keeps organizations at the forefront of technological advancements.

6.7. Security and Risk Mitigation

Distributing workloads across multiple cloud environments enhances security by reducing the impact of a potential security breach. Additionally, organizations can implement diverse security measures provided by different cloud vendors, creating a layered defense strategy.

6.8. Flexibility in Technology Stacks

Different cloud providers offer varied technology stacks and AI frameworks. A multi-cloud strategy provides the flexibility to choose the most suitable tools and frameworks for specific use cases, promoting diversity and adaptability in technology adoption.

6.9. Disaster Recovery and Business Continuity

Multi-cloud environments facilitate robust disaster recovery and business continuity plans. Organizations can ensure rapid recovery in case of a disaster or system failure by having data and applications replicated across different clouds.

6.10. Adaptability to Changing Business Needs

The dynamic nature of a multi-cloud AI strategy enables organizations to adapt quickly to changing business requirements. Whether scaling up during peak demand or adopting new AI technologies, the flexibility inherent in a multi-cloud approach accommodates evolving needs.

7. Challenges

While integrating AI in multi-cloud management offers numerous advantages, it has challenges.

7.1. Data Privacy

Since AI algorithms need many data to work, it is crucial to be careful about data privacy. Organizations must pay attention to how they handle and process data to follow privacy regulations.

For instance, an AI system that looks at user behavior for load balancing must do this without breaking privacy rules. It is about using AI responsibly while keeping people's data private and following the law.

7.2. Algorithm Bias

If AI algorithms are not appropriately trained, they can make unfair decisions. This is a big worry, especially regarding deciding how to use resources or cut costs. For example, suppose an AI system is taught using data mostly from one cloud provider. In that case, it might make choices that favor that provider, even if another offers better services or lower prices. It is important to train AI moderately to avoid these biases.

7.3. Complexity

Using AI-driven solutions to manage multiple clouds can be tricky and might take some time for IT professionals to get the hang of it. Organizations may need to invest in training their existing staff or even bring in specialists who are experts in handling these advanced systems. It is about ensuring that the people responsible for managing these technologies are well-prepared and have the right skills.

7.4. Cost of AI Integration

Although AI can lead to cost savings over time, it is essential to recognize that the initial investment for integrating AI into multi-cloud management can be quite significant. Organizations should consider this substantial upfront cost when planning their budgets for multi-cloud strategies. It is about understanding that the benefits may take some time to offset the initial expenses.

7.5. Ethical Reflections

Using AI in decision-making processes raises ethical concerns, particularly about data privacy and algorithmic bias. Organizations must set clear ethical guidelines for using AI in multi-cloud management. This ensures that decisions made by AI systems align with ethical standards, protect user privacy, and avoid biases that could lead to unfair outcomes. It is about making sure that the use of AI is not only effective but also responsible and ethical.

8. Conclusion

Multi-cloud security will continue evolving to meet changing business and security requirements. One development area will be the increased use of artificial intelligence and machine learning to automate security tasks and enhance threat detection and remediation. Additionally, containers and serverless computing are expected to increase in multi-cloud environments, requiring new security measures to protect these technologies. As multi-cloud environments become more complex, the potential threats also grow, creating a larger area that needs strong and consistent security solutions. This means that security measures and policies must be effective and uniform across all computing environments, whether on-premises, in the cloud, or at the edge. It is about ensuring a solid and consistent defense against threats in every part of the computing landscape.

Organizations exploring multi-cloud security solutions should look for a solution provider with a proven track record of implementing and maintaining multi-cloud security solutions. It is important that any potential solution provider also regularly update their security intelligence and controls to ensure they are aligned with the evolving threat landscape and industry best practices. Securing data and applications in various cloud setups is complex, and the strategic importance of AI in strengthening these digital landscapes is emphasized. The shift from traditional security methods to the dynamic integration of AI technologies represents a fundamental

change in how organizations deal with cybersecurity in the age of multi-cloud computing. As organizations increasingly leverage the benefits of multi-cloud architectures for flexibility, scalability, and operational efficiency, the imperative to fortify these environments becomes more pronounced. The nuanced challenges of interoperability, data governance, and unified identity management in a multi-cloud AI landscape are acknowledged, emphasizing the need for holistic security approaches. The advantages of this symbiotic relationship between multi-cloud security and AI range from redundancy and high availability to cost optimization and innovation. This has provided actionable insights into crafting a secure multi-cloud network, addressing network segmentation, encryption, and continuous monitoring considerations. The multifaceted nature of securing a multi-cloud environment requires a strategic, adaptive, and collaborative approach that aligns with the principles of AI-driven innovation. In essence, "Multi Cloud Security with AI" propels organizations into the future of cybersecurity, where intelligence, adaptability, and collaboration converge to safeguard digital assets across diverse cloud landscapes. This white paper serves as a guide to understanding the intricacies of multi-cloud security and as a blueprint for organizations looking to embrace the opportunities presented by multi-cloud architectures with confidence and resilience. The dynamic fusion of multi-cloud security with AI is not just a response to the challenges of today but a proactive stance towards the evolving digital landscape of tomorrow.

References

[1] Matt Wallace, Multi-Cloud in the world of AI, Dataversity, 2023. [Online]. Available: https://www.dataversity.net/multi-cloud-in-the-world-of-ai/

[2] C3.ai, Multi Cloud, 2022. [Online]. Available: https://c3.ai/glossary/artificial-intelligence/multi-cloud/

[3] f5, What Is Multi-Cloud Security?, 2024. [Online]. Available: https://www.f5.com/glossary/multi-cloud-security

[4] Cross4Cloud, The Future of Multi-Cloud Management: The Role of Artificial Intelligence, 2023. [Online]. Available: https://cross4cloud.com/cloud-corner/blog/the-future-of-multi-cloud-management-the-role-of-artificial-intelligence/

[5] Dana Petcu, "Multi-Cloud: expectations and current approaches," *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds*, pp. 1-6, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[6] Paul Sinai, Artificial Intelligence Projects Can Benefit from the Multi-Cloud, Medium, 2021. [Online]. Available: https://towardsdatascience.com/why-organizations-should-consider-multi-cloud-for-ai-and-how-to-make-it-happen-d9849757b09c

[7] Jiangshui Hong et al., "An Overview of Multi-Cloud Computing," *Web, Artificial Intelligence and Network Applications*, pp. 1055-1068, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nicolas Ferry et al., "Managing Multi-Cloud Systems with CloudMF," *Proceedings of the Second Nordic Symposium on Cloud Computing & Internet Technologies*, pp. 38-45, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hamza Ali Imran et al., "Multi-Cloud: A Comprehensive Review," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Lea Ethan, "Multi-Cloud Management: Orchestrating and Securing Distributed Cloud Environments," *Department of Computer Science, University of Cambridge*, pp. 1-9, 2023. [Google Scholar] [Publisher Link]

[11] Tahir Alyas et al., "Multi-Cloud Integration Security Framework Using Honeypots," *Mobile Information Systems*, vol. 2022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Prakash Somasundaram "Enhanced Security in Multi-Cloud Environments through Federated Access Control," *International Journal of Computer Engineering & Technology*, vol. 14, no. 2, pp. 90-96, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. K. Yakoob, and V. Krishna Reddy "Efficient Identity-Based Multi-Cloud Security Access Control in Distributed Environments," *International Journal of e-Collaboration (IJeC)*, vol. 19, no. 3, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jason Lingle et al., "Security-as-a-Service in a Multi-Cloud Environment," pp. 1-10, 2019. [CrossRef] [Google Scholar]

[15] Rinkey Singh, and Raino Bhatia, "AI Cloud Computing in Education," *International Journal of Research in Science and Engineering*, vol. 3, no. 4, pp. 37-42, 2023. [CrossRef] [Publisher Link]

[16] Abid Ali et al., "AI-Enabled Cloud Security Based on Organized Identity System," 2022. [Google Scholar]

[17] Jo Debecker, Using AI to Optimize a Multi-Cloud Strategy, AI Business, 2023. [Online]. Available: https://aibusiness.com/verticals/using-ai-to-optimize-a-multi-cloud-strategy

[18] Rahul Phadke, The Importance of AI in the Enterprise and How to Build a Secure Multi-Cloud Network, F5, 2023. [Online]. Available: https://www.f5.com/company/blog/the-importance-of-ai-in-the-enterprise-and-how-to-build-a-secure-multi-cloud-network

[19] Codemotion, Why Choose a Multi-cloud Strategy for AI Deployment, 2023. [Online]. Available: https://www.codemotion.com/magazine/ai-ml/multi-cloud-strategy-for-ai/

[20] Cisco, Multicloud Security: Architecture and Ultimate Guide, 2024. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/multicloud-security-architecture.html

[21] CheckPoint, What is Multi-Cloud Security. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-multi-cloud-security/

[22] Wiz Experts Team, Multi Cloud Security Explained, 2024. [Online]. Available: https://www.wiz.io/academy/multi-cloud-security