 ISSN ONLINE 2067-5704

DATA SECURITY IN HYBRID CLOUD INFRASTRUCTURES

Marius TODERICI[1], Diana Cristina DRAGOMIR[2], Mircea Claudiu FULEA[3], Mihai DRAGOMIR[4] and Aurel Mihail TITU[5,6]

[1]National University of Science and Technology Politehnica Bucharest, Bucharest, Romania, ORCID No. 0009-0007-6065-6502, marius@toderici.ro
[2] Technical University of Cluj-Napoca, ORCID No. 0000-0001-6833-8815, diana.dragomir@muri.utcluj.ro
[3] Technical University of Cluj-Napoca, ORCID No. 0000-0001-9640-6379, mircea.fulea@staff.utcluj.ro
[4] Technical University of Cluj-Napoca, ORCID No. 0000-0003-0561-4274, mihai.dragomir@muri.utcluj.ro
[5]Lucian Blaga University of Sibiu, Sibiu, Romania, Corresponding author, ORCID No. 0000-0002-0054-6535, mihail.titu@ulbsibiu.ro
[6]Academy of Romanian Scientists, 3 Ilfov Street, Bucharest, Romania

ABSTRACT: Hybrid cloud infrastructures, which integrate on-premises resources with public cloud services, provide organizations with significant benefits in terms of scalability and cost efficiency. However, this architectural model also introduces complex challenges related to data security and governance. This article examines the primary security risks inherent to hybrid cloud environments and proposes a set of technical and organizational measures aimed at ensuring compliance with the Confidentiality, Integrity, and Availability (CIA) triad. The study emphasizes the critical role of Identity and Access Management (IAM) through the adoption of centralized platforms integrated with Multi-Factor Authentication (MFA) and Single Sign-On (SSO) mechanisms, enabling granular access control and enhanced operational traceability. Furthermore, the paper analyses the importance of implementing Privileged Access Management (PAM) solutions to secure administrative accounts and mitigate risks associated with excessive or abused privileges. Particular attention is devoted to data protection strategies, including end-to-end encryption based on widely accepted standards such as TLS 1.3 for data in transit and AES-256 for data at rest. Finally, the article underscores the necessity of adopting the Zero Trust security model, complemented by advanced monitoring and analytics solutions such as SIEM, EDR, and UEBA, to establish a resilient security posture capable of addressing modern cyber threats.

KEYWORDS: hybrid cloud, cloud security, authentication, identity management, zero trust

DOI 10.56082/annalsarscieco.2026.3.41

1. INTRODUCTION

In an ever-evolving digital landscape, adopting hybrid cloud infrastructures (Figure 1) has become a strategic necessity for organizations seeking to balance the agility of public cloud providers with the rigorous control of on-premises resources. This mixed architecture offers major competitive advantages in terms of scalability and cost optimization, but it also brings with it complex security and data governance challenges. The central objective of this article is to analyze the fundamental mechanisms necessary to ensure the CIA triad (confidentiality, integrity, and availability) in such an environment.

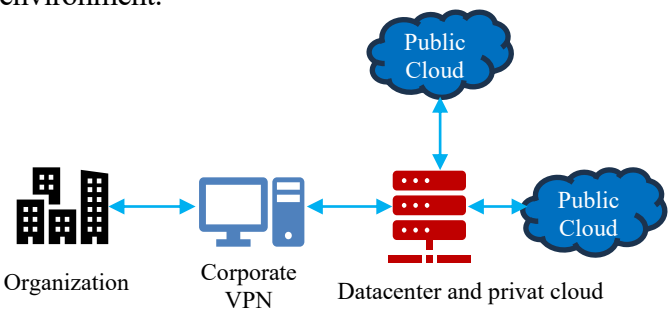

Figure 1. Figure 1 Hybrid Cloud

Through a multidimensional approach, we will explore the essential pillars of a modern security strategy: from rigorous identity and access management (IAM) and the implementation of Zero Trust architectures to advanced encryption and data classification techniques. In an era where the traditional network perimeter is disappearing, security can no longer be a peripheral element, but must become the foundation on which the entire hybrid infrastructure is built.

2. SECURITY IN HYBRID CLOUD INFRASTRUCTURES

The security of hybrid cloud environments is a key aspect of modern IT infrastructures, as these architectures integrate the resources and services offered by public cloud providers with the organization's internal (on-premises) infrastructure. This combination offers significant benefits in terms of flexibility, scalability, and cost optimization, but introduces high complexity in terms of control and governance over data, applications, and communications [1].

Therefore, a hybrid cloud environment requires a unified, consistent, and adaptable security framework that enables consistent enforcement of protection policies across all levels of the architecture. The fundamental objective of implementing advanced security mechanisms is to ensure the confidentiality, integrity, and availability of information—known as the CIA triad (Confidentiality, Integrity, Availability) [2]. To achieve this goal, organizations must adopt a multidimensional approach that includes prevention, detection, response, and recovery measures, integrated into a unified governance strategy. A key part of this strategy is Identity and Access Management (IAM), which gives you granular control over user access and helps you apply the principle of least privilege. By implementing centralized IAM solutions, combined with multi-factor authentication (MFA) and single sign-on (SSO) mechanisms, organizations can prevent unauthorized access and increase the traceability of activities [3].

In addition, privileged access management (PAM) is becoming essential for protecting accounts with extensive administrative rights, as these are the most vulnerable and pose the highest security risk. Data security is also a strategic priority in hybrid environments. Data must be encrypted both in transit, using secure protocols (such as TLS 1.3), and at rest, using strong encryption algorithms such as AES-256. Managing encryption keys through an internally controlled Key Management Service (KMS) provides an additional level of security. At the same time, classifying data according to sensitivity level and applying differentiated access policies are recommended by international standardization bodies [4]. At the same time, the implementation of Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) ensures organizational resilience.

From a networking and communications perspective, security must be strengthened through segmentation and micro-segmentation, reducing the attack surface and limiting the spread of internal threats. Connections between on-premises and cloud infrastructures must be made through secure channels (e.g., VPN, AWS Direct Connect, Azure ExpressRoute), accompanied by the implementation of next-generation firewalls (NGFW), intrusion detection and prevention systems (IDS/IPS), and measures to protect against DDoS attacks [5].

Continuous monitoring and detection is another essential pillar of hybrid cloud security. Centralizing and correlating logs through a Security Information and Event Management (SIEM) system enables real-time analysis of security events, while Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions provide active protection for servers and workstations. In addition, User and Entity Behavior Analytics (UEBA) facilitates the proactive identification of abnormal activities based on deviations from normal usage patterns [6].

Vulnerability management and patching play an important role in maintaining infrastructure resilience. This includes regular scans of infrastructure and applications, prompt application of updates, and regular testing through penetration exercises. Such a proactive approach minimizes the risk of known vulnerabilities being exploited and supports the adoption of a security-oriented organizational culture. Governance and compliance form the foundation of a sustainable security strategy. Defining and applying clear security policies, combined with the use of Cloud Security Posture Management (CSPM) tools, ensures monitoring and automation of compliance with international regulations (such as GDPR, ISO/IEC 27017, NIST SP 800-53). Regular audits and reporting to the organization's management help maintain a unified view of the security posture and continuously improve processes [4].

3. IDENTITY AND ACCESS

Identity and access management in hybrid cloud environments has become a strategic solution for organizations seeking to combine the flexibility and scalability of public cloud services with the control and security of their own infrastructures. From this point of view, the use of IAM solutions is vital for proper user management. The integrated hybrid cloud infrastructure is complex and can generate reluctance for users if they have to enter passwords or authenticate themselves in each system. Thus, this integration poses major challenges in the field of information security, particularly in terms of identity and access management (IAM), a critical component for maintaining trust and compliance [1]. Identity and access management (IAM) is the foundation of a coherent security environment in hybrid cloud architectures. Its purpose is to ensure that only authorized users, applications, and devices can access the right resources at the right times and under well-defined conditions. In an environment where applications and data can be distributed across multiple cloud providers (such as AWS, Azure, or Google Cloud), centralizing identity management becomes essential to maintaining complete visibility into access and associated events.

A practical example is an organization that uses Microsoft Azure for storage services and on-premises infrastructure for internal applications. It can

implement Azure Active Directory (Azure AD) as a centralized IAM solution. By integrating Azure AD with on-premises systems through Azure AD Connect, all user accounts are synchronized, enabling single sign-on and the application of the same access policies regardless of resource location. This significantly reduces the risk of inconsistency between cloud and on-premises environments. An effective IAM system must provide secure authentication and granular authorization. Multi-factor authentication (MFA-Figure 2) is an essential requirement, as most cyber-attacks target user accounts. Combining a password with a temporary code generated on a mobile device or a physical security key provides additional protection. Integration with single sign-on (SSO) solutions also simplifies the user experience.

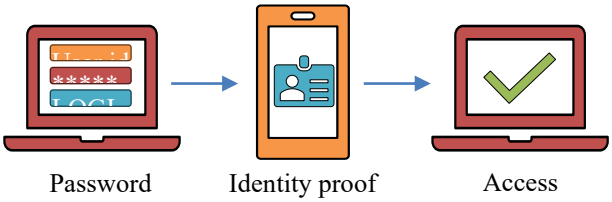

Figure 2. Multi-factor authentication (MFA)

For example, an employee using Okta Identity Cloud can access internal and external applications with a single sign-on, reducing the risk of password reuse. Applying the principle of least privilege is a fundamental best practice. For example, in a software development company, test engineers should not have access to production environments, and system administrators should only have temporary access when necessary. Platforms such as AWS Identity and Access Management (IAM) allow you to define detailed policies that specify exactly what actions a user can perform on each AWS service.

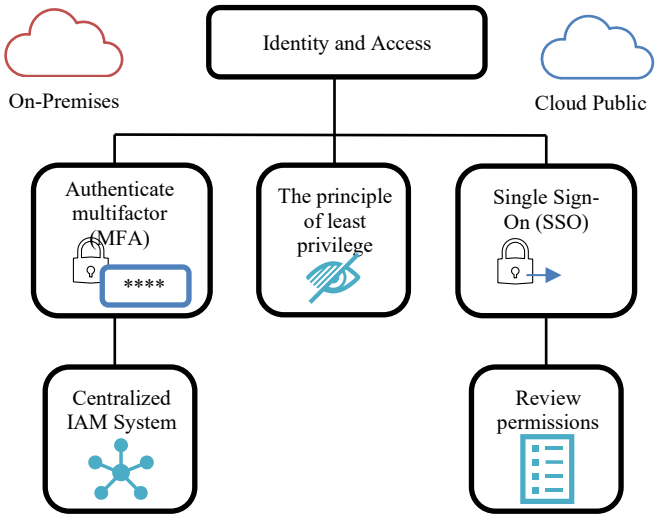

Figure 3. The role of IAM in hybrid cloud infrastructure

Privileged Access Management (PAM) is an extension of IAM that focuses on controlling accounts with administrative privileges. These accounts, which can modify infrastructure or security policies, represent one of the biggest vulnerabilities in a hybrid system. For example, organizations using AWS and VMware can implement CyberArk PAM or BeyondTrust to control administrators' access to servers. Each privileged session is logged and monitored, and passwords are automatically rotated after each use. In Microsoft environments, the Entra Privileged Identity Management (PIM) solution allows temporary access to be granted, preventing abuse by different roles in the system.

IAM integrates with other security solutions, forming a coherent protection ecosystem. For example, connecting IAM with a SIEM system, such as Splunk or IBM QRadar, allows authentication events to be correlated with other types of security incidents. Adopting the Zero Trust architecture, as recommended by NIST SP 800-207, means that no entity is considered trustworthy by default. IAM becomes a mechanism for continuous authentication and authorization, evaluating the context and behavior of the user. A banking institution implementing the Zero Trust model in Azure can use Microsoft Defender for Identity and conditional access policies to block access from unsecured devices. The IAM system (Figure 3) works with the UEBA engine to identify anomalies, such as simultaneous logins from two different locations. In conclusion, identity and access management (IAM) is central to the security strategy in hybrid cloud environments. Its effective implementation provides granular control, increased visibility into user activities, and a significant reduction in risk. By integrating IAM solutions with MFA, SSO, and PAM mechanisms, organizations can build a modern security architecture that complies with Zero Trust principles and international compliance standards [4]. Practical examples show that using solutions such as Azure AD, AWS IAM, Okta, CyberArk, or Microsoft PIM not only simplifies access management but also strengthens the organization's cyber resilience.

4. DATA SECURITY

Data security is a central pillar of hybrid cloud architectures, as data is at the core of any organizational activity and has significant strategic value. In a hybrid context where information is distributed between on-premises environments and public or private cloud environments, data protection becomes a necessity. This involves not only technical mechanisms such as encryption or access control, but also governance, classification, and disaster recovery

processes. In a comprehensive approach, data security in the hybrid cloud includes (Figure 4):

- encryption of data in transit and at rest;
- key management system (KMS);
- classification and differentiated access control;
- implementation of backup mechanisms and recovery plans (DRP/BCP).

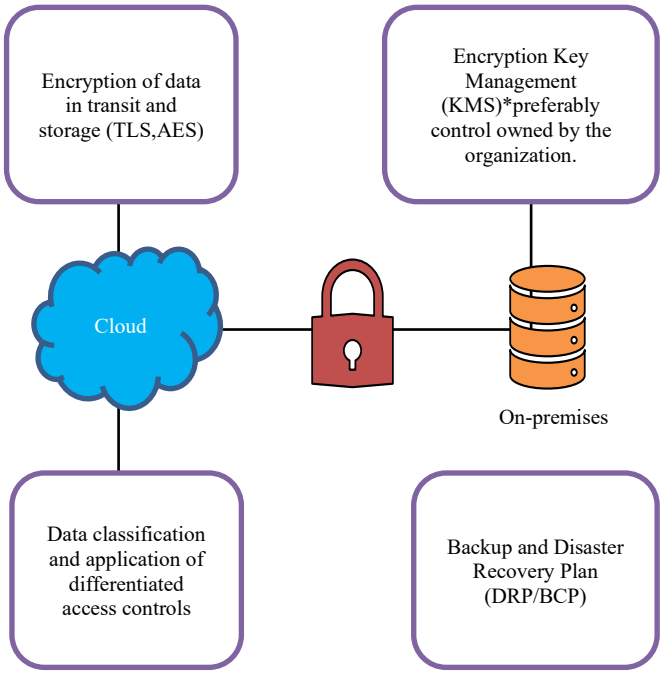

Figure 4. Data security in hybrid cloud infrastructures

5. ENCRYPTION OF DATA IN TRANSIT AND AT REST

Encryption is one of the most important data protection measures because it ensures the confidentiality and integrity of information, even if the infrastructure or communication channels are compromised. In a hybrid cloud environment, data constantly moves between internal networks and external platforms, which requires constant end-to-end protection.

Data encryption in transit - This refers to protecting data that is transmitted between systems, applications, or users.

Modern encryption protocols are used, such as:

- TLS 1.3 (Transport Layer Security) – to protect web traffic between clients and servers;
- IPsec VPN – for secure tunnels between the on-premises and cloud environments;
- SSH or SFTP – for secure file transfers.

Practical example - An organization that synchronizes customer data between internal servers and a database hosted in AWS uses VPN with IPsec and TLS 1.3 to prevent attackers from intercepting data during transmission.

Data encryption at rest (in storage) - Encryption of data "at rest" (in storage) protects information stored on disks, databases, containers, or cloud volumes. Strong algorithms such as AES-256 (Advanced Encryption Standard), considered the industry standard by NIST, are typically used.

Major cloud providers such as AWS, Azure, and Google Cloud implement automatic encryption of data stored in their services (EBS, S3, Blob Storage, Cloud Storage). However, organizations can also apply an additional level of encryption at the application level.

Practical example – An organization can encrypt data stored in Azure Blob Storage using keys generated through Azure Key Vault, ensuring the protection of sensitive data even in the event of unauthorized access to the cloud infrastructure. The same can be done in on-premises infrastructure or with information stored in databases. This is recommended in all cases, as it protects stored information, including from employees with administrative rights, because even though they have elevated rights that allow them to access information, they will not have the keys to decrypt the stored information, thus ensuring data confidentiality, one of the most important pillars of CIA.

6. KEY MANAGEMENT SERVICE (KMS)

Although encryption is essential, its effectiveness depends directly on cryptographic key management. If a key is lost, compromised, or reused incorrectly, all encrypted data becomes vulnerable. Therefore, it is vital for organizations to implement a Key Management Service (KMS).

Key management models:

- Cloud provider-managed KMS – the provider offers automated key generation, rotation, and secure storage services (e.g., AWS KMS, Azure Key Vault, Google Cloud KMS).
- Bring Your Own Key (BYOK) – the organization creates and manages its own keys, but imports them into the cloud infrastructure, retaining full control over the encryption process.
- Hold Your Own Key (HYOK) – keys do not leave the on-premises environment; access to data in the cloud is only possible with the explicit approval of the organization.

Benefits of an effective KMS:

- Complete control over the key lifecycle;
- Full logging and auditability;
- Compatibility with internal policies and compliance requirements (e.g., GDPR, ISO/IEC 27018).

Practical example in an organization: the IT department uses AWS KMS with the BYOK model, generating keys in its own internal HSM (Hardware Security Module). Thus, AWS cannot access encrypted data without the company's explicit approval.

7. DATA CLASSIFICATION AND DIFFERENTIATED ACCESS CONTROLS

In modern hybrid cloud infrastructures, data is central to organizational processes and constitutes a particularly valuable strategic resource. However, not all data is equally important or sensitive. Some data may be public or operational, while other data may contain critical financial, personal, or government information. Therefore, data classification becomes a fundamental step in security management, with the aim of establishing the appropriate way to protect, access, and handle information.

The data classification process is methodical and involves a comprehensive analysis of the types of information an organization holds, their value, and the associated risks. The main steps include identifying data types, assessing sensitivity levels, and labeling with appropriate controls. Identifying data types involves taking inventory of the information managed:

- personal data – information about employees, partners (names, social security numbers, biometric data);
- financial data – transactions, balance sheets, bank details;
- operational data – information about internal processes, flows, departmental activities;
- technical data – source code, hardware configurations, infrastructure diagrams, IT configurations.

This classification allows for a clear understanding of the data that is essential to the functioning of the organization and that which requires additional protection. The assessment of sensitivity is performed by analysing the potential impact of unauthorized disclosure, loss, or modification of data. Financial, reputational, operational, and legal impacts are considered. High-risk data is given priority in security policies. Labeling and applying appropriate controls involves assigning a classification level to each category of data: public, internal, confidential, and critical.

Table 1. Data categories and protection levels

Date Category	Description	Level of protection	Example
Public	Freely distributed data with no impact on security	No restrictions	Web pages, contact details, press releases
Internal	Data used in current internal activities	Authenticating standards	Work procedures, internal reports
Confidential	Sensitive data, disclosure moderately affects the organization	Encryption, MFA, strict IAM policies	Financial documents, source code
Critical	Data critical to the security of the organization	Advanced encryption, restricted access, SIEM monitoring	Medical data, bank transactions

Each level is associated with specific policies ranging from access control to encryption and monitoring requirements. In accordance with ISO/IEC 27001 and NIST SP 800-60 recommendations, an effective classification can be structured according to Table 1. This structure allows for the application of a proportional protection model, avoiding both over-protection of non-critical information and exposure of sensitive information.

Data classification must be complemented by access controls appropriate to the level of risk. These controls can be technical, administrative, or procedural, designed to limit access to authorized persons only. Multi-factor authentication (MFA) is essential for protecting sensitive data, combining passwords with additional factors such as temporary codes or physical devices. Role-based access policies (RBAC) and Identity and Access Management (IAM) systems ensure that users are only granted the rights they strictly need, in accordance with the "least privilege" principle. Access monitoring and auditing is performed by Security Information and Event Management (SIEM) solutions, which analyse logs in real time to detect unusual activity. Data Loss Prevention (DLP) solutions also prevent the unauthorized transmission of sensitive information via email, cloud applications, or external devices.

Data classification and differentiated access controls are the foundation of an effective security strategy in hybrid cloud environments. They enable organizations to identify, protect, and monitor information based on its importance, ensuring a balance between security, performance, and compliance.

8. CONCLUSIONS

Securing hybrid cloud infrastructures must be approached as a continuous, adaptive, and holistic process that extends beyond the implementation of isolated technical controls. The inherent complexity of this architectural model - characterized by the distribution of workloads across on-premises environments and public cloud platforms - necessitates an integrated security strategy capable of addressing operational requirements alongside

governance and compliance obligations. Within this framework, the coherent integration of Identity and Access Management (IAM) solutions, the enforcement of strict encryption policies, and the implementation of a rigorous data classification scheme constitute foundational components of an effective security posture. These controls must be governed by the principle of least privilege and aligned with the Zero Trust security model, which eliminates implicit trust and requires continuous verification of identities, devices, and access contexts. As demonstrated throughout this study, the adoption of mature technologies such as Azure Active Directory, AWS Key Management Service, and Privileged Access Management (PAM) solutions enables organizations to maintain consistent visibility, accountability, and control over sensitive data, regardless of where it is stored or processed. Furthermore, the NIS 2 Directive underscores the importance of proactive risk management, incident detection, and response capabilities. In this regard, the integration of continuous monitoring, security event correlation, and incident response mechanisms ensures compliance with requirements related to threat handling, operational continuity, and service availability. Ultimately, cyber resilience in hybrid cloud environments is determined by an organization's ability to align security governance, regulatory compliance, and executive accountability with effective technical controls and organizational processes. By adopting internationally recognized security standards and fostering a security-oriented culture, hybrid cloud infrastructures can function not only as enablers of innovation but also as resilient and compliant platforms for the protection of essential and important digital services under the NIS 2 regulatory framework.

9. REFERENCES

[1] NIST., Zero Trust Architecture, NIST Special Publication 800-207, Vol. II, pag. 1-50, Gaithersburg, MD, (2023).

[2] ISO/IEC., Information Security, *Cybersecurity and Privacy Protection*, *ISO/IEC 27001*, Vol. 2022, No. 1, pag. 1-48, (2022).

[3] Gartner., *Identity and Access Management in Hybrid Environments*, Research Series, Gartner Inc. eds., Stamford, CT, (2023).

[4] ENISA., *ENISA Cloud Security Guide for SMEs, 2nd edition*, European Union Agency for Cybersecurity eds., Athens, Greece, (2024).

[5] Cisco., *Hybrid Cloud Security Report, 1st edition*, Cisco Systems eds., San Jose, CA, (2023).

[6] Microsoft Security, *Extended Detection and Response (XDR) in Hybrid Clouds*, Cloud Security Journal, Vol. 2024, No. 4, pag. 10-25, (2024).

[7] Kandula, S. R. (2025). *Emerging security challenges and AI-driven solutions in multi-cloud and hybrid environments.* Journal of Recent Trends in Computer Science and Engineering, 13(1),89–98. https://doi.org/10.70589/jrtcse.2025.13.1.11

[8] Mostafa, S. (2025). *Cloud security & compliance: A conceptual roadmap for organizations.* International Journal on Science and Technology, 4(9).https://www.ijsat.org/papers/2025/4/9207.pdf

[9] Waseem, M., et al. (2025). *SDN-enabled adaptive security framework for multi-cloud infrastructures using deep learning-based threat detection and policy management.* PeerJ Computer Science, https://doi.org/10.7717/peerj-cs.3266

[10] Zhang, Y., & Li, X. (2025). *BC2P-1305: An enhanced data security in cloud computing network using blockchain based ChaCha20-Poly1305 cryptography*. Frontiers in Blockchain, https://doi.org/10.3389/fbloc.2025.1636056

[11] Titu, M. A., Deac-Suteu, D., Toderici, M. I., *Catalogul de Servicii Informatice – Instrument pentru Îmbunătățirea Calității și Securității Suportului Informatic într-o Companie*, Acta Technica Napocensis, Cluj-Napoca, Romania, (2021).

[12] Majumdar, S., Madi, T., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L., Debbabi, M., *Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack*, International Conference on Cloud Computing Technology and Science (CloudCom), IEEE eds., Vancouver, Canada, (2015).

[13] Banciu, D., *Cercetare – Dezvoltare – Inovare prin Soluții Cloud*, Mobile Innovation 2015, Bucharest, Romania, (2015).

[14] Banciu, D., *Infrastructură de Tip Cloud pentru Instituțiile Publice din România – ICIPRO*, Big Data, The Cloud, Analytics – Triunghiul Profitabilității, București, Romania, (2016).

[15] Guida, G. C., Limongiello, M., An Evolved *Bridge Digital Twin Framework: A New Paradigm for Infrastructure Monitoring and Management*, Lecture Notes in Networks and Systems, vol. 1484, Springer eds., Sarajevo, Bosnia and Herzegovina, (2025).

[16] Polinati, A., K., *Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments*, Cryptography and Security, arXiv:2506.00426, (2025).