Exploring Opportunities and Challenges in Multi-Cloud and Hybrid Cloud Implementation: A Focus on Security and Data Management

Wigananda Firdaus Putra Aditya [a,1], Anjik Sukmaaji [a,2]

[a] Magister Teknologi Informasi UPN "Veteran" Jawa Timur, Jl.Raya Rungkut Madya, Surabaya 60294,Indonesia
[b] Fakultas Teknologi dan Informatika Universitas Dinamika, Jl. Raya Kedung Baruk 98, Surabaya 60298, Indonesia

[1]wiganandafirdaus@gmail.com; [2]anjik@dinamika.ac.id

ARTICLE INFO

ABSTRACT

Keywords
Cloud Computing
Multi Cloud
Hybrid Cloud
Cloud Solution
Zero Trust

This study explores the opportunities and challenges of implementing multi-cloud and hybrid cloud models, with a specific focus on security and data management. While multi-cloud environments offer organizations flexibility and reduced dependence on single providers, they introduce complex security and privacy challenges due to the need to manage data across multiple platforms. Hybrid cloud models, integrating both public and private clouds, offer the advantage of retaining sensitive data on-premises while leveraging public cloud scalability. To address these challenges, advanced security measures such as Homomorphic Encryption and Hybrid Cryptosystems, combining DES and RSA algorithms, are discussed for their potential to secure data without sacrificing accessibility. The Zero Trust model, which assumes all networks are inherently hostile, is also highlighted as essential for reinforcing security in cloud environments. This literature review underscores the importance of comprehensive, multi-layered security policies—from infrastructure to application layers—to protect sensitive data within complex cloud setups. Effective data management strategies, supported by robust encryption and security policies, are essential for organizations aiming to maximize the benefits of cloud computing while maintaining strong security. This study offers valuable insights into how organizations can strategically implement secure, flexible cloud solutions

1. Introduction

A lot of companies are now using cloud technology to work together better. Basically, digital tech has made businesses more modern and streamlined [1]. As cloud computing continues to advance, enterprises must stay abreast of the latest developments and trends in cloud strategies, ensuring that their decisions remain informed and relevant [2]. IT integrates services from different cloud providers, and integrates hybrid cloud systems Integration of infrastructure and services, emphasizing the flexibility and scalability that today's businesses require As organizations navigate this complex terrain is clear that there is no one-size-fits-all solution [3]. From the explanations above, it can be concluded that companies implement cloud technology to facilitate better collaboration. Information Technology can integrate services from various cloud providers, where the integration of cloud systems emphasizes flexibility and scalability to meet the evolving needs of businesses. This means that the implementation of cloud computing is not a one-size-fits-all solution.

As digital transformation accelerates, a growing number of organizations are adopting cloud computing to enhance collaboration, scalability, and operational efficiency. Cloud computing offers businesses unprecedented flexibility, allowing them to scale resources as needed and access a wide range of services on-demand. The advent of multi-cloud and hybrid cloud models, where organizations use multiple cloud providers and integrate both private and public cloud infrastructures, has significantly advanced this flexibility. However, with these innovations come new complexities and challenges, especially in managing security and data integrity across different environments.

Multi-cloud and hybrid cloud approaches are becoming the preferred strategies for enterprises seeking to avoid vendor lock-in, optimize performance, and enhance resilience by diversifying across multiple cloud services. According to recent studies, over 80% of organizations are pursuing multi-cloud strategies to balance workload demands and meet regulatory requirements. This shift is driven by the need for robust infrastructure that can support various applications while maintaining stringent data security and compliance standards. For instance, hybrid cloud allows organizations to retain sensitive data on-premises in private clouds while leveraging public cloud resources for less critical workloads, creating a balanced infrastructure that maximizes the benefits of both models.

However, this blend of public and private clouds introduces challenges that require a nuanced approach to security and data management. In multi-cloud environments, data security is a paramount concern as organizations must protect sensitive information across multiple platforms with differing security standards. As each cloud provider has unique configurations, ensuring consistent security measures can be difficult, and organizations must adopt a strategic approach to minimize vulnerabilities. Advanced security models like Zero Trust, along with sophisticated encryption techniques such as Homomorphic Encryption and Hybrid Cryptosystems, are becoming essential to safeguard data in these complex environments.

Given the rapid growth in cloud technology, there is an urgent need for businesses to understand the implications of multi-cloud and hybrid cloud models. This paper aims to explore the opportunities these models offer while analyzing the associated security and data management challenges. By reviewing current literature on cloud implementation strategies, this study provides insights into how organizations can develop resilient and secure multi-cloud and hybrid cloud infrastructures.

2. Method

The preparation of this paper follows a systematic literature review methodology, carefully designed to capture a comprehensive view of current developments, challenges, and best practices in multi-cloud and hybrid cloud implementation with a focus on security and data management. The research methodology consists of several sequential steps: literature search, filtering, categorization, data extraction, and qualitative analysis.

2.1 Literature Search

The literature search focused on identifying high-quality, peer-reviewed articles and studies relevant to multi-cloud and hybrid cloud implementations, specifically concerning security and data management. This search was conducted across multiple academic and research databases, including Google Scholar, IEEE Xplore, ScienceDirect, and ResearchGate. To ensure the results reflected current knowledge and technological advancements, the search was limited to studies published within the last ten years (2013-2023). Key search terms included “Multi-Cloud,” “Hybrid Cloud,” “Cloud Security,” “Cloud Data Management,” “Zero Trust,” and “Homomorphic Encryption,” among others. Searches were also conducted with various combinations of keywords to maximize the discovery of relevant literature.

2.2 Filtering and Categorization

After compiling an initial list of studies, a thorough filtering process was applied to refine the selection. Each study was evaluated based on several criteria: relevance to multi-cloud or hybrid cloud implementation, focus on security and data management, and methodological rigor. Articles were excluded if they did not specifically address cloud security or data management issues, or if they were limited to vendor-specific solutions that lacked generalizability. Additionally, articles published in languages other than English were excluded to maintain consistency and accessibility. Only studies indexed in reputable international journals were considered, ensuring that the sources met a high standard of academic integrity and reliability.

2.3 Categorization and Data Extraction

The selected articles were then categorized into thematic groups to facilitate a structured literature review. Key themes included:

- Introduction to Cloud Computing: General overview of cloud computing models, including multi-cloud and hybrid cloud.
- Cloud Computing Architecture: Exploration of architectural considerations in cloud environments, with a focus on multi-cloud and hybrid configurations.
- Cloud Security Techniques: Detailed analysis of security practices in cloud computing, covering encryption methods, Zero Trust principles, and access control mechanisms.
- Data Management in Cloud Computing: Examination of data storage, management, and sharing in multi-cloud and hybrid cloud setups.
- Advanced Security and Encryption Techniques: Focus on recent technological advancements in data security, such as homomorphic encryption and hybrid cryptosystems.

Data extraction involved summarizing each study's primary findings, methodologies, proposed solutions, and identified gaps. This process enabled a structured comparison of different approaches, challenges, and proposed innovations across the literature

2.4 Qualitative Analysis:

Following categorization, a qualitative analysis was performed to synthesize insights from the literature. This analysis aimed to identify recurring patterns, trends, and divergences in the implementation of multi-cloud and hybrid cloud systems, particularly in the areas of security and data management. An inductive approach was used to allow themes to emerge organically from the data, which helped highlight both widely accepted practices and emerging solutions. This process also involved comparing and contrasting the findings of various studies to reveal any contradictions, limitations, or areas where further research is needed.

2.5 Limitations

The scope of this literature review was limited to peer-reviewed articles and studies in English, indexed in reputable international journals. This decision was made to maintain consistency in quality and relevance but may limit the inclusion of some regional studies or non-English language research. Additionally, vendor-specific white papers and non-academic publications were excluded, as these sources often lack rigorous peer review and may introduce bias. The focus was also restricted to recent developments in multi-cloud and hybrid cloud security, excluding studies that do not specifically address these aspects.

2.6 Ethical Considerations

As this study is a literature review, ethical considerations primarily involved ensuring proper citation and representation of authors' ideas and findings. All sources were referenced accurately to respect intellectual property and avoid misinterpretation.

By following this systematic approach, this study aims to provide a well-rounded and objective view of the opportunities and challenges in multi-cloud and hybrid cloud environments, emphasizing both established security practices and innovative strategies.

3. Results and Discussion

This chapter will discuss the results of the analysis that has been carried out on the journals that have been filtered and categorized previously. This discussion focuses on the opportunities and challenges of multi-cloud and hybrid cloud implementation. This includes a discussion of Cloud security data management and Advanced Technologies in multi cloud and hybrid cloud.

In implementing Hybrid Cloud technology, organizations can take advantage of the advantages of public and private clouds. Organizations that need to benefit from private and public Clouds can take advantage of hybrid models. Hybrid Cloud aims to reduce the inherent limitations of purely public and private approaches by combining them into a multi-Cloud that harnesses its strengths[4]. This overcomes the limitations of using one type of cloud by combining the advantages of multi clouds and hybrid clouds. The statement above is also strengthened by the other statement A Multi hybrid cloud model allows organizations to provide, use, and manage IT resources across their private cloud set-ups and any compatible public cloud[5]. From the statement above, it can be concluded that in implementing cloud computing, companies can implement both multi-cloud and hybrid cloud models simultaneously. Hybrid cloud combines the use of public and private clouds simultaneously while implementing multi-cloud can involve the use of several different public cloud providers.

In implementing Multi Cloud Computing, the security side must also be a special concern. Multi-cloud environments offer flexibility and scalability but introduce significant security and privacy challenges. Encryption techniques, access control mechanisms, and compliance measures are essential for mitigating risks and ensuring data protection[6]. One of the data security techniques in cloud computing is the application of Homomorphic Encryption. Homomorphic Encryption is a technique in cryptography that is used to encrypt plaintext using one or more algebraic operations.[7]. Other research on security also reveals that the implementation of homomorphic encryption can ensure a high level of security in a multi-cloud environment. This technique allows data processing without decryption, keeping the data secure from potential breaches during the process[8]. From the opinions above, it can be interpreted that the implementation of multi-cloud greatly helps organizations in carrying out their activities, but security challenges must also be a special concern. Several security-related innovations in cloud computing have been tried in previous studies, from these results homomorphic is one of the data security methods that can be an alternative in implementing cloud computing. Homomorphic was chosen because it can enable secure data processing without sacrificing data confidentiality by utilizing encryption methods with comprehensive access.

Another studies also discuss how to secure multi-cloud and hybrid cloud environments. Attacks targeting cloud computing platforms are highly dynamic, which means it is more important to implement intrusion prevention systems rather than merely detecting intrusions. In practice, this can be achieved using several approaches based on statistical methods, knowledge, and machine learning[9]. In the implementation of multi cloud, several recent studies have revealed that security is very important. Other studies on security in multi cloud say that in the implementation of multi cloud, the Zero Trust principle can also be applied. Zero Trust network model is a modern network security model that aims to solve challenges introduced by modern technology and workplace structures. It is built around some basic assumptions, the primary of which is that the network is always hostile[10]. With the Zero Trust Model of information security, attackers have a harder time getting into your network and having a harder time wreaking havoc once inside[11]. From previous research, it can be concluded that the implementation of multi-cloud can be assumed that the network has a nature that is never safe. So that in the implementation of zero trust attackers will be more difficult to enter and damage the network. The zero trust approach can be applied with statistical-based methods, or machine learning. Cloud security must be implemented at all layers, from physical infrastructure to the application and data layers. Multi-cloud service providers need to have a comprehensive security policy, including identity management, access control, and data encryption to protect information from rapidly evolving threats[12].

In the implementation of multi cloud and hybrid cloud that is easy is by changing the way to manage and store data in the organization. With many cloud providers through various storage, data management in this environment is becoming increasingly complex. The data management process in multi cloud and hybrid cloud certainly has its own challenges. this has also been helped by the many cloud service providers that have supported various data storage and management models. Effective data management is certainly very important to be able to provide prime effects in multi cloud and hybrid cloud environments. Experimental results have shown that Multi-Cloud Storage using a Hybrid Crypto System is the optimal choice for data sharing[13]. This is because the Hybrid Crypto system uses a combination of 2 encryption techniques including Triple DES and RSA. Other studies related to data management in cloud computing were also conducted and it can be concluded that the proposed hybrid cryptosystem-based architecture effectively mitigates threats from insiders and malicious users, achieving high levels of efficiency and flexibility [14].

4. Conclusion

This review has examined the advantages, challenges, and security requirements associated with multi-cloud and hybrid cloud implementations, with a focus on data management and security. Multi-cloud and hybrid cloud models offer organizations significant benefits, including enhanced flexibility, scalability, and a reduction in vendor lock-in. By using multiple cloud providers, organizations can optimize their IT infrastructure for performance and resilience, while hybrid models allow sensitive data to remain on-premises in private clouds, reducing exposure to potential external threats.

However, implementing these cloud strategies introduces complex challenges in ensuring consistent and robust security. The review highlights that security in multi-cloud and hybrid cloud environments must be addressed holistically—covering all layers from infrastructure to applications. Techniques such as Homomorphic Encryption and Hybrid Cryptosystems provide promising solutions for protecting sensitive data across cloud environments, enabling secure data processing without compromising confidentiality. Additionally, the Zero Trust security model emerges as essential for mitigating threats in environments where traditional network boundaries are no longer sufficient. By adopting a Zero Trust approach, organizations can better defend against internal and external threats, improving resilience in these increasingly complex cloud ecosystems.

Despite advancements in security methods, integrating and managing multiple cloud environments remains challenging, particularly in ensuring interoperability, compliance, and effective data management. Effective implementation of multi-cloud and hybrid cloud systems requires a well-defined strategy that includes comprehensive security policies, continuous monitoring, and investment in skilled personnel. As cloud computing technology continues to evolve, future research should explore scalable encryption techniques, automated security management, and machine learning-driven intrusion prevention methods that can further protect and streamline multi-cloud and hybrid cloud environments.

In conclusion, while multi-cloud and hybrid cloud approaches offer significant flexibility and growth potential, they demand sophisticated security and data management strategies to realize their benefits fully. Organizations adopting these models must prioritize both advanced security protocols and ongoing strategic planning to navigate the inherent complexities. Continued innovation and rigorous research in cloud security and management practices are essential to enabling organizations to leverage the full potential of these cloud models while safeguarding their data and operations.

References

[1] M. Attaran, “Cloud Computing Technology: Leveraging the Power of the Internet to Improve Business Performance,” *J. Int. Technol. Inf. Manag.*, vol. 26, no. 1, pp. 112–137, Jan. 2017, doi: 10.58729/1941-6679.1283.

[2] A. Panteli, “Examining Poly-Cloud in Enterprise Cloud Strategies : Differentiating Between Multi-Cloud and Hybrid Cloud Approaches,” vol. 13, no. 1, pp. 22308849012023–02, 2023.

[3] S. Shrivastava and Y. Agrawal, “Multi-Cloud Deployments and Hybrid Cloud Architecture,” *Resmilitaris*, vol. 10, no. 1, pp. 4754–4760, 2024, doi: 10.48047/resmil.v10i1.16.

[4] D. Zeginis *et al.*, “A user-centric multi-paas application management solution for hybrid multi-cloud scenarios,” *Scalable Comput.*, vol. 14, no. 1, pp. 17–32, 2013, doi: 10.12694/scpe.v14i1.824.

[5] A. J. Ferrer, D. G. Pérez, and R. S. González, “Multi-cloud Platform-as-a-service Model, Functionalities and Approaches,” *Procedia Comput. Sci.*, vol. 97, pp. 63–72, 2016, doi: 10.1016/j.procs.2016.08.281.

[6] N. Mohammad, “Multi-Cloud Environments : a Comprehensive Study on Encryption Techniques and Access Control,” no. April, 2024.

[7] A. R. Anggoro, “Studi Mengenai Fully Homomorphic Encryption dan Perkembangannya dari RSA sebagai Enkripsi Homomorfis Populer,” 2018.

[8] O. Zibouh, A. Dalli, and H. Drissi, “Cloud computing security through parallelizing fully Homomorphic encryption applied to multi-cloud approach,” *J. Theor. Appl. Inf. Technol.*, vol. 87, no. 2, pp. 300–307, 2016.

[9] H. H. Naqvi, T. Alyas, N. Tabassum, U. Farooq, and A. Namoun, “Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 3, pp. 2533–2539, 2021, doi: 10.30534/ijatcse/2021/1451032021.

[10] J. Flanigan, “Zero Trust Network Model,” pp. 1–7, 2018, [Online]. Available: https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf

[11] V. N. S. S. Chimakurthi, “The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment,” *ABC J. Adv. Res.*, vol. 9, no. 2, pp. 89–102, 2020, doi: 10.18034/abcjar.v9i2.608.

[12] S. Achar, “Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape,” *World Acad. Sci. Eng. Technol. Int. J. Comput. Syst. Eng.*, vol. 16, no. 9, pp. 379–384, 2022, doi: 10.5281/zenodo.7084251.

[13] K. Subramanian and F. L. John, “Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system,” *Int. J. Adv. Appl. Sci.*, vol. 5, no. 1, pp. 15–23, 2018, doi: 10.21833/ijaas.2018.01.003.

[14] K. Subramanian and F. L. John, “Secure and Reliable Unstructured Data Sharing in Multi-Cloud Storage using the Hybrid Crypto System,” vol. 17, no. 6, pp. 196–206, 2017.