Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

(REVIEW ARTICLE)

Reimagining multi-cloud interoperability: A conceptual framework for seamless integration and security across cloud platforms

Sunday Adeola Oladosu [1,*], Adebimpe Bolatito Ige [2], Christian Chukwuemeka Ike [3], Peter Adeyemo Adepoju [4], Olukunle Oladipupo Amoo [5] and Adeoye Idowu Afolabi [6]

[1] *Independent Researcher, Texas, USA.*
[2] *Independent Researcher, Canada.*
[3] *Globacom Nigeria Limited.*
[4] *Independent Researcher, Lagos, Nigeria.*
[5] *Amstek Nigeria Limited.*
[6] *CISCO, Nigeria.*

Open Access Research Journal of Science and Technology, 2022, 04(01), 071–082

Publication history: Received on 02 January 2022; revised on 11 February 2022; accepted on 14 February 2022

Article DOI: https://doi.org/10.53022/oarjst.2022.4.1.0026

Abstract

The rapid adoption of multi-cloud environments by organizations is driven by the need for greater flexibility, cost optimization, and risk mitigation. However, achieving seamless interoperability across multiple cloud platforms remains a significant challenge. This review proposes a conceptual framework designed to facilitate smooth integration and robust security within multi-cloud environments, aiming to overcome existing barriers such as data silos, platform dependencies, and inconsistent security policies. The framework emphasizes a unified approach to managing cross-cloud data flow, application interoperability, and performance optimization while ensuring end-to-end security. The framework introduces key components essential for seamless integration, including centralized data management and orchestration tools, standardized APIs, and middleware that enable consistent communication across diverse cloud providers. It also highlights the importance of designing applications with cross-cloud capabilities using containerization and microservices. Additionally, the framework addresses the need for continuous performance monitoring and optimization, ensuring that resources are efficiently managed across platforms. On the security front, the review presents a unified security model that spans across multiple clouds, leveraging Zero Trust architecture and advanced encryption techniques. Real-time threat detection, automated security management, and compliance monitoring are integral aspects of the proposed framework, enabling proactive and consistent security enforcement. By adopting this approach, organizations can safeguard sensitive data, comply with regulatory requirements, and mitigate security risks in dynamic multi-cloud environments. This conceptual framework not only enhances the interoperability and efficiency of multi-cloud infrastructures but also fosters a more secure, scalable, and future-proof cloud environment. The review concludes with an exploration of real-world case studies and industries that benefit from this integrated approach, as well as the future evolution of multi-cloud interoperability driven by AI, automation, and edge computing technologies.

Keywords: Multi-Cloud interoperability; Seamless integration; Cloud platforms; Conceptual framework

1. Introduction

In recent years, the adoption of multi-cloud strategies has significantly increased within modern enterprises (Reinartz et al., 2019). Multi-cloud refers to the use of multiple cloud computing services from different providers, instead of relying on a single cloud platform. This shift has been driven by the desire for greater flexibility, risk mitigation, and cost optimization. Companies are no longer limited to one provider's offerings; instead, they can choose the best services from different clouds based on their specific needs, such as performance, cost, and geographic availability (Attaran and

* Corresponding author: Sunday Adeola Oladosu.

Woods, 2019; Tricomi et al., 2020). Furthermore, multi-cloud adoption allows organizations to avoid vendor lock-in, which reduces dependence on a single provider and provides better control over cloud infrastructure.

The rise of multi-cloud strategies is also a response to the evolving digital landscape, where businesses are increasingly leveraging cloud solutions for various aspects of operations, from data storage and processing to application hosting (Chakraborty, 2019; Tomarchio et al., 2020). The diversification of cloud platforms enables organizations to take advantage of specialized features offered by different cloud service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). As enterprises move towards digital transformation, multi-cloud environments offer the scalability, agility, and resilience required to meet complex business demands and to stay competitive (Mazilescu, 2020).

While multi-cloud adoption provides numerous benefits, it also introduces several challenges that organizations must navigate. One of the main complexities is managing the integration and orchestration of multiple cloud platforms (Sivathapandi et al., 2021). Each cloud service provider offers different tools, APIs, and management frameworks, making it difficult for enterprises to create a unified management structure. This fragmentation can lead to inefficiencies, increased operational overhead, and potential delays in application deployment. Interoperability is another critical challenge in multi-cloud environments. The lack of standardized protocols and the variability in cloud architectures complicate data sharing and communication across different platforms (Alli and Alam, 2020). Organizations may struggle with data synchronization, consistency, and availability, which can lead to silos of information, hindering collaboration between cloud services. Security is a further concern, as ensuring robust protection across diverse platforms requires complex configuration and management. Different security policies, compliance standards, and encryption methods across cloud providers can increase the risk of vulnerabilities, making it harder for organizations to implement cohesive security measures across all platforms (Kethireddy, 2021; Akhtar et al., 2021).

To address these challenges, this review proposes a conceptual framework aimed at enhancing multi-cloud interoperability and ensuring seamless integration and robust security. The framework focuses on providing a structured approach to managing the complexity of multi-cloud environments while optimizing performance and minimizing risks. By leveraging standardized tools and protocols, the framework will facilitate smoother communication and data flow between various cloud platforms, promoting greater collaboration and efficiency (Angel et al., 2021). Additionally, it will incorporate security best practices, ensuring that organizations can maintain a consistent level of protection across multiple providers, while adhering to regulatory requirements and industry standards. The goal of this framework is to help organizations transition smoothly to a multi-cloud strategy by offering guidelines on how to effectively manage and integrate various cloud services, while also ensuring high levels of security and reliability. As multi-cloud environments continue to evolve, this framework will provide a roadmap for enterprises to navigate the complexities of managing multiple cloud platforms, paving the way for more scalable, agile, and secure cloud infrastructures (Gade, 2021; Awaysheh et al., 2021).

2. Current State of Multi-Cloud Environments

Multi-cloud environments refer to the use of multiple cloud computing services from different cloud providers, where organizations employ a combination of private and public cloud platforms to meet diverse operational requirements (Kritikos et al., 2019). These environments allow enterprises to optimize their IT infrastructure by selecting specific cloud services based on performance, cost, compliance, and scalability needs. Key characteristics of multi-cloud architectures include flexibility, redundancy, and the ability to avoid vendor lock-in. Rather than relying on a single cloud provider, organizations can distribute their workloads and services across multiple clouds, reducing the risks associated with platform dependence. Common multi-cloud models include hybrid cloud, which integrates both private and public cloud environments to offer greater flexibility, security, and control. In hybrid cloud architectures, sensitive data and critical workloads are managed within a private cloud, while less critical tasks can be run on public clouds. Another popular model is the use of public and private cloud combinations, where organizations use public clouds for scalability and cost efficiency while maintaining private clouds for more secure, high-compliance operations. This type of architecture enables businesses to optimize their cloud strategies according to specific use cases, balancing performance, security, and cost concerns across different cloud platforms.

While multi-cloud environments provide numerous benefits, they also introduce a range of integration challenges (Hong et al., 2019). One of the most significant issues is data siloing, where data becomes fragmented across different cloud platforms, making it difficult to achieve a cohesive, real-time view of information. Data may be stored in different formats or structures, creating difficulties in accessing and sharing information between cloud providers. Furthermore, inconsistent APIs across various clouds pose challenges in orchestrating and automating workloads, as each platform

may require different tools and processes to manage resources, resulting in increased operational overhead. Vendor lock-in is another issue inherent in multi-cloud environments. While multi-cloud architectures aim to reduce dependency on a single provider, it can still be difficult to fully eliminate vendor lock-in, particularly when integrating proprietary solutions or services offered by individual cloud providers. Vendor-specific technologies and tools often create dependencies that can make it challenging to migrate workloads seamlessly between clouds. Additionally, cross-platform communication becomes complex due to the absence of universal standards for cloud service integration (Blanco and Lucrédio, 2021). This lack of interoperability makes it harder for organizations to effectively connect and manage multiple cloud platforms, leading to inefficiencies and higher costs.

Security is one of the foremost concerns in multi-cloud environments. Organizations often struggle to maintain consistent data security across different platforms, as each cloud provider may have unique security models, encryption standards, and access controls. As a result, organizations may find it difficult to enforce uniform security policies across multiple clouds, increasing the risk of vulnerabilities. Moreover, compliance challenges arise when different cloud providers adhere to varying regulatory standards, which may differ based on geographic regions or industry-specific requirements (Mubarkoot and Altmann, 2021). Organizations operating across jurisdictions must ensure that their multi-cloud strategies comply with relevant laws and regulations, which can be a complex and resource-intensive process. Inconsistent security policies across clouds add another layer of complexity to managing security in multi-cloud environments. For example, a cloud provider's built-in security features might not align with those of another provider, leaving gaps in protection. This inconsistency can lead to security loopholes, making it harder for organizations to monitor, control, and mitigate potential threats across different platforms. Additionally, the growing prevalence of cybersecurity threats in cloud environments, such as data breaches, denial-of-service attacks, and ransomware, highlights the need for a more robust and unified approach to cloud security. Therefore, addressing these security concerns is critical to ensuring the safe and efficient operation of multi-cloud environments. While multi-cloud environments offer flexibility and scalability, they present significant challenges in terms of integration, security, and data management. To fully leverage the benefits of multi-cloud strategies, organizations must navigate these obstacles by developing standardized tools, policies, and security frameworks that enable effective management and integration across diverse cloud platforms.

2.1. Conceptual Framework for Seamless Multi-Cloud Integration

Seamless integration in multi-cloud environments refers to the ability to effectively connect and manage disparate cloud platforms without the friction of incompatibility or inefficiencies (Han et al., 2020). A seamlessly integrated multi-cloud system should provide unified data management, enabling organizations to handle data across multiple clouds as if they were a single entity. This includes ensuring consistency in how data is stored, accessed, and manipulated across platforms. Centralized monitoring is essential for gaining visibility into the performance and health of applications and infrastructure, regardless of which cloud the services are hosted on. Furthermore, cross-cloud collaboration must be facilitated by robust frameworks that allow workflows and processes to span across different cloud environments, thereby enabling streamlined operations and resource management. Key characteristics of seamless integration also include minimizing latency and reducing the complexity of managing multiple cloud platforms simultaneously. The goal is to provide an experience where the end-user or IT administrator does not perceive distinct differences between various cloud environments. To achieve this, organizations must adopt best practices in data governance, security, and automation to enable smooth data flow and application performance across all clouds (Lnenicka and Komarkova, 2019).

A unified data management strategy is fundamental to the success of multi-cloud integration. Centralized data management platforms allow organizations to manage data consistently across multiple cloud platforms. These platforms facilitate data synchronization, transformation, and storage in ways that are compatible with the unique requirements of each cloud provider. For instance, it is necessary to create a centralized repository where data from different sources can be accessed and analyzed efficiently, reducing the risk of data silos. Alongside data management, orchestration tools are vital in automating workflows and coordinating tasks across cloud environments (Corodescu et al., 2021). These tools help synchronize actions between different cloud services, ensuring that the workflows are executed in a controlled, predictable manner. They also enable performance monitoring to detect anomalies and maintain service levels. By automating processes, organizations can avoid manual intervention and reduce the likelihood of errors. The orchestration layer thus plays a central role in ensuring consistency and reliability in multi-cloud environments.

At the heart of seamless integration is the ability to ensure interoperability between various cloud services. Standardized APIs and middleware solutions are essential for this. APIs act as the connectors between different cloud platforms, allowing them to exchange data and communicate with each other effectively. The challenge here lies in the diversity of APIs across providers, as each cloud service may have its own proprietary API. Therefore, adopting

standardized APIs across platforms helps simplify this communication. Middleware solutions also play an important role by acting as an intermediary layer that facilitates the exchange of information between different cloud environments (Bouloukakis et al., 2019). These solutions ensure that disparate systems can function together by converting data into formats that are compatible with different cloud platforms. By using standardized data exchange protocols (such as RESTful APIs or GraphQL) and formats like JSON or XML, middleware solutions ensure that applications and services in different clouds can work seamlessly.

Building applications that can function seamlessly across multiple clouds requires careful design. The architecture must be platform-agnostic, allowing it to operate smoothly regardless of the underlying cloud service. Containerization and microservices are essential technologies for achieving cross-cloud application compatibility. Containers allow developers to package applications and their dependencies into a single, portable unit that can be deployed across different cloud platforms without modification (Watada et al., 2019). Microservices decompose applications into smaller, independent services that can be scaled, updated, or deployed independently. This approach enables cross-cloud compatibility by allowing different microservices to reside on different cloud platforms while maintaining their ability to communicate with each other through APIs. This modular approach reduces the complexity of maintaining monolithic applications and supports flexibility in choosing the best cloud for each service or component.

Performance monitoring is a crucial component in a seamless multi-cloud framework. It allows organizations to continuously track the performance of applications and cloud resources across all platforms in real-time. Tools for monitoring must be able to track service metrics, such as response times, availability, and resource utilization, regardless of which cloud platform is hosting the service. These tools must offer cross-platform visibility to provide comprehensive insights into system performance. Additionally, load balancing and resource optimization mechanisms must be implemented to ensure that cloud resources are used efficiently across platforms (Zhang et al., 2020). Load balancing helps distribute incoming traffic evenly across cloud environments to avoid overloading a particular platform, ensuring consistent service delivery. Optimizing resource usage ensures that workloads are dynamically adjusted to the most suitable cloud provider based on factors such as cost, performance, and geographical location.

A conceptual framework for seamless multi-cloud integration must incorporate unified data management, standardized APIs and middleware, cross-cloud application development, and performance monitoring (Ramalingam and Mohan, 2021). These components work together to create an interconnected, flexible, and efficient multi-cloud environment. As organizations continue to adopt multi-cloud strategies, a well-designed integration framework will be critical to ensuring consistent performance, operational efficiency, and data security across diverse cloud platforms.

2.2. Enhancing Security in Multi-Cloud Environments

The adoption of multi-cloud environments introduces several significant security challenges, primarily stemming from the inherent complexity of managing diverse cloud platforms. One of the most pressing issues is the difficulty in enforcing consistent security policies across different cloud providers. Each cloud service provider typically has its own security protocols, encryption standards, access controls, and governance frameworks (Ali et al., 2020). This disparity makes it difficult for organizations to implement a uniform security posture across all cloud platforms, leading to potential gaps in protection. As a result, organizations may face challenges in monitoring and maintaining security consistency, which can increase the risk of security breaches or misconfigurations. Another critical security challenge is data privacy concerns, especially in light of varying regional regulations. Different countries and regions have distinct data privacy laws and compliance requirements, such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the United States. When data is distributed across multiple clouds, each with different geographical locations and legal jurisdictions, it becomes increasingly difficult for organizations to ensure that their data handling practices are in compliance with all applicable laws. Failure to adhere to these regulations can result in legal consequences, reputational damage, and financial penalties.

To address these challenges, organizations must adopt a unified security model that spans across all cloud platforms, enabling them to manage security policies and controls in a centralized and cohesive manner. A centralized security framework would provide a single point of visibility and control over the security posture of all cloud environments. This approach facilitates consistent enforcement of security policies, such as access management, encryption, and incident response, across diverse cloud infrastructures. By integrating all cloud platforms into a single security framework, organizations can minimize the risk of security gaps that arise from managing disparate cloud services (Alouffi et al., 2021). One effective strategy in securing multi-cloud environments is the adoption of a Zero-trust architecture. In a Zero-trust model, no user, device, or application is trusted by default, regardless of whether they are inside or outside the network perimeter. This approach ensures that every access request is thoroughly authenticated and authorized before granting access to sensitive resources. Zero-Trust helps mitigate the risks associated with cross-

cloud communication by continuously validating trustworthiness and minimizing the attack surface. It provides a robust framework for managing security in complex, distributed environments, such as those found in multi-cloud configurations. In addition to Zero-Trust, advanced encryption techniques are vital for securing sensitive data in transit and at rest across multiple cloud platforms. End-to-end encryption ensures that data remains protected throughout its lifecycle, whether it is being transferred between cloud environments or stored on servers. Encrypting data not only safeguards it from unauthorized access but also provides an added layer of security for compliance with data privacy regulations. Secure authentication mechanisms, such as multi-factor authentication (MFA), should also be integrated into the security framework to ensure that only authorized users or systems are granted access to cloud resources (Kebande et al., 2021).

Given the dynamic and complex nature of multi-cloud environments, automated security management is essential for maintaining real-time protection. Leveraging AI and machine learning (ML) can significantly enhance threat detection, incident response, and adaptive security measures. AI-driven tools can analyze vast amounts of data across cloud platforms to identify abnormal patterns or potential security threats in real time. Machine learning algorithms can continuously learn from historical attack data, improving the system's ability to predict and mitigate emerging threats. Automated incident response systems can take immediate action based on pre-defined rules, such as isolating compromised systems or triggering alerts, thus reducing the response time and minimizing damage. Furthermore, automated security tools can help streamline compliance monitoring and enforcement. Regulatory compliance in multi-cloud environments requires continuous oversight to ensure that all security controls and data management practices align with industry standards and legal requirements (Khalil, 2020). Automated compliance tools can regularly audit cloud environments, generate compliance reports, and notify administrators of any deviations from required standards. By automating these processes, organizations can reduce the administrative burden of compliance management and ensure that they remain aligned with regulatory expectations. The integration of automated security solutions into multi-cloud environments allows organizations to respond more quickly and efficiently to threats while maintaining a high level of security across complex infrastructures. Moreover, automation enables continuous monitoring and adjustment of security protocols, making it easier to keep up with evolving threats and compliance demands.

Enhancing security in multi-cloud environments requires a comprehensive approach that addresses the unique challenges posed by distributed architectures. By adopting a unified security model, incorporating Zero-Trust principles, and leveraging advanced encryption techniques, organizations can improve the protection of their cloud resources. Additionally, automated security management using AI and machine learning can enable real-time threat detection and adaptive security, ensuring that multi-cloud environments remain secure and compliant. As the complexity of multi-cloud infrastructures continues to grow, these strategies will play a critical role in safeguarding sensitive data and maintaining robust security across diverse cloud platforms (Alenezi, 2021).

2.3. Benefits of the Conceptual Framework

A conceptual framework for multi-cloud environments offers significant improvements in interoperability and flexibility, allowing businesses to fully leverage the strengths of multiple cloud platforms without compromising on integration. Traditionally, multi-cloud architectures have been challenged by the difficulty of ensuring seamless communication and data exchange between different cloud providers. However, a well-designed framework facilitates the integration of heterogeneous cloud platforms by providing standardized protocols, data models, and interfaces. This enables businesses to access a variety of cloud services and tools, including those that cater to specialized needs, without being locked into a single provider. By supporting interoperability, the framework empowers organizations to choose the best features of each cloud service, such as storage, computing power, and machine learning capabilities, to optimize their operations and performance (Hassan and Mhmood, 2021). This flexibility ensures that businesses can adapt to evolving technological advancements and changing business requirements without being constrained by a single cloud provider's limitations.

The adoption of a conceptual framework also contributes to streamlined operations and cost efficiency by optimizing multi-cloud resource management. In a multi-cloud environment, managing resources across different platforms can quickly become complex, requiring significant manual intervention and oversight. However, a conceptual framework enables centralized management of resources, automating tasks such as load balancing, resource allocation, and data synchronization. This reduces the administrative burden and the risk of errors, allowing IT teams to focus on higher-value activities. Moreover, by optimizing resource usage across various clouds, businesses can avoid over-provisioning and underutilization, both of which can lead to unnecessary costs. The framework helps to ensure that the right resources are available at the right time, thereby reducing waste and improving overall operational efficiency (Dev et al., 2020). Cost optimization also extends to the ability to select the most cost-effective cloud services, ensuring that businesses only pay for the resources they need, without sacrificing performance or scalability.

A unified conceptual framework strengthens the security and compliance posture of multi-cloud environments by providing proactive security measures and ensuring consistent governance across platforms. Security in multi-cloud environments can be challenging due to varying security policies, tools, and configurations across different providers (Sharma, 2020). However, the framework establishes a cohesive security model, ensuring that the same standards and controls are applied across all clouds. By integrating Zero-trust architecture, encryption protocols, and identity management, businesses can enforce consistent security measures, protecting sensitive data and preventing unauthorized access. Furthermore, the framework simplifies compliance with industry standards and regulations, such as GDPR, HIPAA, and PCI DSS, by ensuring that all cloud environments adhere to the necessary legal and security requirements. With built-in tools for auditing, monitoring, and reporting, businesses can maintain continuous oversight and stay compliant with minimal manual effort.

One of the key benefits of the conceptual framework is its ability to support scalability and future-proofing in cloud environments. As organizations grow and their computing needs evolve, they must be able to scale their cloud infrastructures efficiently. Traditional single-cloud solutions may impose limitations in terms of resources or geographical availability, restricting a business's ability to expand (Barika et al., 2019). However, a multi-cloud framework facilitates the seamless scaling of resources across multiple platforms, allowing businesses to expand their infrastructure as needed. This scalability is particularly important for businesses that are experiencing rapid growth or entering new markets, as it enables them to add resources from different providers without disruption. Moreover, the framework is designed to be future-proof, allowing businesses to integrate new technologies such as 5G, artificial intelligence, and edge computing as they emerge. This ensures that organizations remain agile and adaptable in the face of technological advancements, without being locked into a single cloud provider's roadmap.

The conceptual framework for multi-cloud environments offers a variety of significant benefits, including improved interoperability, streamlined operations, enhanced security, and scalability. By enabling seamless integration of different cloud platforms, businesses can optimize their resource management, reduce operational complexity, and lower costs (George and Karunakaran, 2021). The framework's proactive security measures ensure robust protection and compliance across all cloud environments, while its scalability features provide the flexibility needed for future growth. In a rapidly changing technological landscape, the framework empowers businesses to remain agile, adaptable, and prepared for the challenges and opportunities that lie ahead.

2.4. Case Studies and Industry Applications

Several organizations across various industries have successfully implemented multi-cloud strategies, leveraging frameworks designed to enhance interoperability, resource optimization, and security (Chelliah and Surianarayanan, 2021). One prominent example is Netflix, which utilizes a multi-cloud architecture to ensure global availability and scalability. By combining Amazon Web Services (AWS) with Microsoft Azure and Google Cloud, Netflix can provide uninterrupted service to its millions of global users. The integration of multiple cloud platforms allows Netflix to balance workloads, handle spikes in demand, and maintain redundancy for disaster recovery purposes. This multi-cloud strategy helps Netflix avoid vendor lock-in, ensuring flexibility and improved service delivery, which aligns with its business goals of reliability, performance, and customer satisfaction. Similarly, General Electric (GE) has adopted a multi-cloud approach for its industrial IoT platform, Predix. GE uses both private and public cloud solutions to process the massive amounts of data generated by industrial equipment across various sectors such as aviation, healthcare, and energy. The multi-cloud architecture provides GE with a scalable, secure environment that supports its diverse data processing and analytics needs. By integrating cloud services from multiple providers, GE can ensure the flexibility to switch between platforms, depending on cost, performance, and regulatory requirements (Li et al., 2021). This allows the company to mitigate risks related to vendor dependency while optimizing its cloud infrastructure to meet evolving business demands.

Different industries are increasingly benefiting from enhanced multi-cloud interoperability and security, addressing the unique challenges they face. In finance, organizations such as JP Morgan Chase have embraced multi-cloud strategies to optimize data storage, risk management, and compliance. Multi-cloud platforms allow financial institutions to diversify their cloud service providers, ensuring that sensitive financial data remains secure and compliant with international regulations like GDPR and MiFID II. The integration of various cloud platforms facilitates the smooth flow of data while adhering to security protocols that protect customer data and ensure high availability during market fluctuations (Galiveeti et al., 2021). In the healthcare sector, organizations like Medtronic and Pfizer are leveraging multi-cloud systems to store and analyze patient data while complying with healthcare regulations such as HIPAA. A multi-cloud framework enables healthcare providers to use the best tools available from different cloud providers, ensuring efficient data storage, accessibility, and real-time processing. Furthermore, these frameworks enhance collaboration between healthcare teams across different regions, facilitating quicker decision-making and improving patient outcomes. The

added layer of security ensures that sensitive health information remains protected from cyber threats, maintaining compliance with stringent data protection standards. In the e-commerce sector, companies such as Amazon and eBay rely on multi-cloud systems to ensure seamless customer experiences, particularly during peak shopping seasons like Black Friday or Cyber Monday. By integrating multiple cloud providers, e-commerce platforms can ensure high performance, low latency, and global reach. Multi-cloud architectures also provide the necessary flexibility to scale infrastructure and handle the massive amounts of transactional data generated during high-demand periods. The security benefits of multi-cloud systems also help mitigate potential cyber threats and safeguard customer payment information, which is critical in maintaining trust in the online retail environment (Akinrolabu et al., 2019).

These case studies demonstrate that businesses across various sectors are reaping the benefits of multi-cloud integration, optimizing performance, security, and compliance while reducing vendor dependency. The flexibility and scalability provided by multi-cloud architectures allow industries like finance, healthcare, and e-commerce to better address their unique challenges, resulting in improved operational efficiencies and enhanced customer satisfaction.

2.5. Implementation Strategies

Implementing a conceptual framework for enhancing multi-cloud interoperability requires a well-structured and methodical approach (Di Francesco et al., 2019). The following step-by-step guide outlines the essential stages for businesses transitioning to multi-cloud environments. The first step is to conduct a comprehensive assessment of the organization's current IT infrastructure, including cloud service usage, data management practices, and security measures. This phase involves identifying existing challenges such as data silos, platform dependencies, and security gaps. A clear understanding of business objectives and the desired outcomes from adopting a multi-cloud strategy should be established. Based on the business requirements, the next step is to define the multi-cloud architecture that best suits the organization’s needs. This includes selecting appropriate public and private cloud services, deciding on the deployment models (e.g., hybrid or multi-cloud), and determining how workloads and data will be distributed across platforms. A critical component of this stage is ensuring that the architecture supports the seamless flow of data and interoperability between clouds. Once the architecture is defined, businesses must create an integration strategy that focuses on connecting the various cloud platforms. This strategy includes selecting tools for data synchronization, API management, and interoperability between cloud environments. Additionally, businesses must decide on the approach for managing security policies, data sharing, and compliance across different platforms. Security is a priority in multi-cloud environments, and this phase involves the implementation of a unified security model. Adopting a Zero-Trust architecture, using encryption technologies, and ensuring compliance with regulatory frameworks are critical actions (Kerman et al., 2020). This stage also involves integrating advanced threat detection systems and ensuring that security measures are consistently applied across all cloud platforms. After deploying the framework, continuous monitoring is essential to ensure the integration is working effectively. This involves tracking performance metrics, identifying any issues with interoperability, and making adjustments as necessary. Optimization tools should be used to fine-tune the multi-cloud setup, ensuring it meets performance, cost, and scalability goals.

To effectively implement the proposed multi-cloud framework, businesses require various tools and technologies that support integration, automation, and management (Imran et al., 2020). Some of the key technologies include. Cloud Management Platforms (CMPs) as VMware vRealize and Cisco CloudCenter allow businesses to manage and monitor multi-cloud environments (Surianarayanan et al., 2019). These platforms offer centralized control for provisioning, managing, and optimizing resources across different cloud providers, helping to simplify multi-cloud operations. Continuous Integration/Continuous Deployment (CI/CD) tools like Jenkins, GitLab CI, and CircleCI are critical for streamlining software development, deployment, and updates in a multi-cloud environment. By automating deployment processes, these tools ensure faster rollouts of applications across different cloud platforms, increasing agility and efficiency. Kubernetes and docker swarm are essential for managing containerized applications across multiple clouds. These platforms provide seamless orchestration, enabling businesses to deploy, scale, and manage containers in hybrid or multi-cloud environments, improving workload portability and operational flexibility. Tools such as Apigee and MuleSoft facilitate API management and integration between disparate cloud services. By using these tools, businesses can create a more streamlined and efficient means of transferring data and integrating services between different platforms (Singu, 2021).

While adopting a multi-cloud framework offers numerous advantages, businesses often encounter several barriers during implementation. These obstacles can be addressed with careful planning and strategic solutions. Many organizations still rely on legacy systems, which may not be compatible with modern multi-cloud environments (Gupta, 2019). The migration of legacy applications to the cloud can be time-consuming and costly. To address this challenge, businesses should prioritize incremental cloud adoption, migrating non-critical applications first, and investing in cloud-compatible infrastructure. Integrating multi-cloud environments with existing on-premises or single-cloud

systems can create interoperability issues. This challenge can be mitigated by adopting hybrid cloud strategies that allow gradual integration and by using middleware solutions to facilitate communication between different systems. Employees and stakeholders may be resistant to the changes required by a multi-cloud adoption strategy. This resistance can be overcome through effective change management strategies, which include training programs, transparent communication about the benefits, and demonstrating the long-term value of a multi-cloud approach. One of the challenges of multi-cloud adoption is avoiding dependency on a single vendor. To mitigate vendor lock-in, businesses should prioritize flexibility in choosing cloud providers, leveraging open-source technologies, and designing their multi-cloud strategy to ensure compatibility with a wide range of cloud services (Park et al., 2020; Bouzerzour et al., 2020).

Implementing a multi-cloud framework requires careful planning, the right tools, and overcoming significant challenges. By following a structured roadmap, leveraging essential technologies, and addressing barriers such as technical debt and integration issues, businesses can successfully adopt multi-cloud strategies that enhance interoperability, security, and cost-efficiency across their operations (Moll and Yigitbasioglu, 2019; Behrendt et al., 2021).

2.6. Future Trends and Evolution of Multi-Cloud Interoperability

The integration of Artificial Intelligence (AI) and automation in multi-cloud environments is set to revolutionize how businesses manage their cloud infrastructures (Gill et al., 2019). AI-driven solutions are expected to enhance interoperability and simplify the management of complex, multi-cloud architectures. One of the key benefits of AI in multi-cloud environments is its ability to automate routine tasks such as resource allocation, data synchronization, and load balancing across multiple cloud platforms (Peralta et al., 2019). By employing AI algorithms, businesses can ensure optimal performance, minimize human error, and reduce operational complexity. Additionally, AI's ability to analyze large datasets and identify patterns will significantly improve decision-making in multi-cloud environments. For example, AI can predict workload demands and automatically adjust resource allocation to meet those needs. Furthermore, machine learning models can be trained to recognize anomalies in cloud operations, such as traffic spikes or security breaches, enabling real-time detection and mitigation of potential issues (Nina and Ethan, 2019). Automation, when integrated with AI, will allow businesses to automate not only operational processes but also security responses, such as patching vulnerabilities or responding to attacks, reducing the burden on IT staff and improving efficiency.

As organizations continue to embrace multi-cloud strategies, cloud security will evolve to address new challenges and risks (Ravi and Thangarathinam, 2019). One of the most pressing issues is ensuring robust encryption and secure data transmission across multiple, often disparate, cloud platforms. Advancements in encryption technologies are expected to play a crucial role in enhancing security in multi-cloud environments (Reddy et al., 2021). Future developments will likely focus on end-to-end encryption methods, where data is encrypted at rest, in transit, and during processing, ensuring its confidentiality and integrity, regardless of the cloud provider. In addition to encryption, identity and access management (IAM) tools will become increasingly sophisticated. The future of IAM in multi-cloud environments will likely see the rise of more granular, policy-driven access control systems, leveraging AI and machine learning to dynamically adjust permissions based on context, such as user behavior, device, and location. This will reduce the risk of unauthorized access, particularly in complex multi-cloud environments. Compliance will also remain a top concern as multi-cloud environments scale (Dubey and Singh, 2019). Future compliance tools will be more automated, using AI to track changes in regulations and ensure that organizations remain compliant across all cloud platforms. Automated auditing and real-time reporting will become standard features, helping organizations to quickly identify compliance gaps and take corrective actions.

The combined power of edge computing and 5G networks will significantly impact multi-cloud interoperability and security in the coming years. Edge computing, which involves processing data closer to the source of generation, will reduce latency and improve real-time processing capabilities, particularly in industries such as manufacturing, healthcare, and autonomous vehicles (Khan et al., 2019). As more devices and applications rely on real-time data processing, edge computing will enable seamless integration across multiple cloud platforms by processing data locally before sending it to the cloud for further analysis. The rise of 5G networks will complement edge computing by providing faster, more reliable connectivity. 5G's low latency and high throughput capabilities will be crucial for multi-cloud environments that require real-time data transfer and processing. This combination of edge computing and 5G will enable businesses to deploy more responsive, dynamic, and scalable applications, thus enhancing multi-cloud interoperability by ensuring that data is processed and shared between cloud environments without the typical delays associated with traditional cloud computing (Kelechi et al., 2019; Bhat et al., 2020). In terms of security, edge computing and 5G networks will introduce new challenges, particularly in terms of data privacy and network security. With data being processed closer to the edge, ensuring secure data transmission between edge devices, multi-cloud platforms, and

end-users will be critical. Advancements in encryption and secure communication protocols will be necessary to maintain data integrity and privacy (Rishu and Sinha, 2021). Additionally, with the proliferation of IoT devices, securing these devices and their interactions with multi-cloud environments will be a priority for businesses looking to protect their networks from vulnerabilities (Tahirkheli et al., 2021).

The future of multi-cloud interoperability is promising, with significant advancements expected in AI, automation, cloud security, and edge computing. AI and automation will streamline management tasks and improve the integration of multiple cloud platforms, while enhanced encryption and IAM technologies will ensure the security and compliance of multi-cloud environments. The convergence of edge computing and 5G will further drive the evolution of multi-cloud systems by enabling real-time data processing and ultra-low latency communication (Angel et al., 2021). These technological advancements will not only improve the efficiency and scalability of multi-cloud architectures but will also create new opportunities for businesses to innovate and optimize their operations in an increasingly connected world.

3. Conclusion

The proposed framework for multi-cloud integration and security offers a structured approach to managing the complexities of multi-cloud environments while ensuring robust security across diverse platforms. Key components of the framework include the centralization of security policies, enabling seamless integration between multiple cloud providers, and the implementation of a unified security model, such as Zero-Trust architecture. These components address critical issues in multi-cloud deployments, including data siloing, interoperability, and platform dependencies. Additionally, the framework emphasizes automation, leveraging AI and machine learning for real-time threat detection, incident response, and compliance monitoring. The benefits of this framework are far-reaching: improved interoperability across cloud platforms, streamlined operations, enhanced security, and cost efficiency. By enabling businesses to optimize resource management and maintain a high level of security, the framework offers a comprehensive solution to the challenges of modern cloud environments.

Looking ahead, the potential of multi-cloud environments is immense. As businesses continue to adopt digital transformation strategies, the need for seamless cloud integration and robust security will only grow. Multi-cloud architectures offer the flexibility to leverage the strengths of different cloud platforms while mitigating risks associated with vendor lock-in and data fragmentation. However, the success of these environments hinges on effective integration strategies and the ability to maintain security across diverse platforms. The future of multi-cloud integration will be shaped by advancements in automation, AI, and edge computing, which will further simplify management and enhance scalability. As organizations strive to stay competitive in an increasingly interconnected world, the ability to seamlessly integrate and secure multi-cloud systems will be a key driver of their success, enabling them to innovate and adapt to changing market demands.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A. and Praveen, S., 2021. A comprehensive overview of privacy and data security for cloud storage. *International Journal of Scientific Research in Science Engineering and Technology*.

[2] Alenezi, M., 2021. Safeguarding Cloud Computing Infrastructure: A Security Analysis. *Computer Systems Science & Engineering*, *37*(2).

[3] Ali, O., Shrestha, A., Chatfield, A. and Murray, P., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), p.101419.

[4] Alli, A.A. and Alam, M.M., 2020. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet of Things*, *9*, p.100177.

[5] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M., 2021. A systematic literature review on cloud computing security: threats and mitigation strategies. *Ieee Access*, *9*, pp.57792-57807.

[6] Angel, N.A., Ravindran, D., Vincent, P.D.R., Srinivasan, K. and Hu, Y.C., 2021. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, *22*(1), p.196.

[7] Angel, N.A., Ravindran, D., Vincent, P.D.R., Srinivasan, K. and Hu, Y.C., 2021. Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, *22*(1), p.196.

[8] Attaran, M. and Woods, J., 2019. Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *31*(6), pp.495-519.

[9] Awaysheh, F.M., Alazab, M., Garg, S., Niyato, D. and Verikoukis, C., 2021. Big data resource management & networks: Taxonomy, survey, and future directions. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2098-2130.

[10] Behrendt, A., De Boer, E., Kasah, T., Koerber, B., Mohr, N. and Richter, G., 2021. Leveraging Industrial IoT and advanced technologies for digital transformation. *McKinsey & Company*, pp.1-75.

[11] Bhat, S.A., Sofi, I.B. and Chi, C.Y., 2020. Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities. *IEEE Access*, *8*, pp.205340-205373.

[12] Blanco, J.Z. and Lucrédio, D., 2021. A holistic approach for cross-platform software development. *Journal of Systems and Software*, *179*, p.110985.

[13] Bouloukakis, G., Georgantas, N., Ntumba, P. and Issarny, V., 2019. Automated synthesis of mediators for middleware-layer protocol interoperability in the IoT. *Future Generation Computer Systems*, *101*, pp.1271-1294.

[14] Bouzerzour, N.E.H., Ghazouani, S. and Slimani, Y., 2020. A survey on the service interoperability in cloud computing: client-centric and provider-centric perspectives. *Software: Practice and Experience*, *50*(7), pp.1025-1060.

[15] Chakraborty, B., Ambi Karthikeyan, S., Chakraborty, B. and Ambi Karthikeyan, S., 2019. The ever-changing landscape of the cloud. *Understanding Azure Monitoring: Includes IaaS and PaaS Scenarios*, pp.1-20.

[16] Chelliah, P.R. and Surianarayanan, C., 2021. Multi-cloud adoption challenges for the cloud-native era: Best practices and solution approaches. *International Journal of Cloud Applications and Computing (IJCAC)*, *11*(2), pp.67-96.

[17] Corodescu, A.A., Nikolov, N., Khan, A.Q., Soylu, A., Matskin, M., Payberah, A.H. and Roman, D., 2021. Big data workflows: Locality-aware orchestration using software containers. *Sensors*, *21*(24), p.8212.

[18] Di Francesco, P., Lago, P. and Malavolta, I., 2019. Architecting with microservices: A systematic mapping study. *Journal of Systems and Software*, *150*, pp.77-97.

[19] Dubey, M. and Singh, K., 2019. Multi-Cloud Management Strategies-A Comprehensive Review. *RES MILITARIS*, *9*(1), pp.289-299.

[20] Gade, K.R., 2021. Migrations: Cloud Migration Strategies, Data Migration Challenges, and Legacy System Modernization. *Journal of Computing and Information Technology*, *1*(1).

[21] Galiveeti, S., Tawalbeh, L.A., Tawalbeh, M. and El-Latif, A.A.A., 2021. Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 329-360). Cham: Springer International Publishing.

[22] George, J.G. and Karunakaran, A.R., 2021. Enabling Scalable Financial Automation in Omni-Channel Retail: Strategies for ERP and Cloud Integration. *Human-Computer Interaction Perspectives*, *1*(2), pp.10-49.

[23] Gill, S.S., Tuli, S., Xu, M., Singh, I., Singh, K.V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U. and Pervaiz, H., 2019. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things*, *8*, p.100118.

[24] Gupta, L., 2019. *Management and security of multi-cloud applications*. Washington University in St. Louis.

[25] Han, J., Park, S. and Kim, J., 2020. Dynamic OverCloud: Realizing microservices-based IoT-cloud service composition over multiple clouds. *Electronics*, *9*(6), p.969.

[26] Hassan, A. and Mhmood, A.H., 2021. Optimizing network performance, automation, and intelligent decision-making through real-time big data analytics. *International Journal of Responsible Artificial Intelligence*, *11*(8), pp.12-22.

[27] Hong, J., Dreibholz, T., Schenkel, J.A. and Hu, J.A., 2019. An overview of multi-cloud computing. In *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019) 33* (pp. 1055-1068). Springer International Publishing.

[28] Imran, H.A., Latif, U., Ikram, A.A., Ehsan, M., Ikram, A.J., Khan, W.A. and Wazir, S., 2020, November. Multi-cloud: a comprehensive review. In *2020 ieee 23rd international multitopic conference (inmic)* (pp. 1-5). IEEE.

[29] Kebande, V.R., Awaysheh, F.M., Ikuesan, R.A., Alawadi, S.A. and Alshehri, M.D., 2021. A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles. *Sensors*, *21*(18), p.6018.

[30] Kelechi, A.H., Alsharif, M.H., Ramly, A.M., Abdullah, N.F. and Nordin, R., 2019. The four-C framework for high capacity ultra-low latency in 5G networks: A review. *Energies*, *12*(18), p.3449.

[31] Kerman, A., Borchert, O., Rose, S. and Tan, A., 2020. Implementing a zero trust architecture. *National Institute of Standards and Technology*, *2020*, pp.17-17.

[32] Kethireddy, R.R., 2021. AI-Driven Encryption Techniques for Data Security in Cloud Computing. *JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE)*, *9*(1), pp.27-38.

[33] Khalil, F., 2020. The landscape from above: Continuous cloud monitoring for continuous assurance. *Cyber Security: A Peer-Reviewed Journal*, *4*(2), pp.182-193.

[34] Khan, W.Z., Ahmed, E., Hakak, S., Yaqoob, I. and Ahmed, A., 2019. Edge computing: A survey. *Future Generation Computer Systems*, *97*, pp.219-235.

[35] Kritikos, K., Zeginis, C., Iranzo, J., Gonzalez, R.S., Seybold, D., Griesinger, F. and Domaschka, J., 2019. Multi-cloud provisioning of business processes. *Journal of Cloud Computing*, *8*, pp.1-29.

[36] Li, Z., Liang, H., Wang, N., Xue, Y. and Ge, S., 2021. Efficiency or innovation?: The long-run payoff of cloud computing. *Journal of Global Information Management (JGIM)*, *29*(6), pp.1-23.

[37] Lnenicka, M. and Komarkova, J., 2019. Developing a government enterprise architecture framework to support the requirements of big and open linked data with the use of cloud computing. *International Journal of Information Management*, *46*, pp.124-141.

[38] Mazilescu, V., 2020. Cloud Migration and Global Digitalization of Business Models. *Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics*, *26*(3).

[39] Moll, J. and Yigitbasioglu, O., 2019. The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *The British accounting review*, *51*(6), p.100833.

[40] Mubarkoot, M. and Altmann, J., 2021. Software Compliance in Different Industries: A Systematic Literature Review. *CIISR@ Wirtschaftsinformatik*, pp.36-51.

[41] Nina, P. and Ethan, K., 2019. AI-Driven Threat Detection: Enhancing Cloud Security with Cutting-Edge Technologies. *International Journal of Trend in Scientific Research and Development*, *4*(1), pp.1362-1374.

[42] Park, J., Kim, U., Yun, D. and Yeom, K., 2020. Approach for selecting and integrating cloud services to construct hybrid cloud. *Journal of Grid Computing*, *18*, pp.441-469.

[43] Peralta, G., Garrido, P., Bilbao, J., Agüero, R. and Crespo, P.M., 2019. On the combination of multi-cloud and network coding for cost-efficient storage in industrial applications. *Sensors*, *19*(7), p.1673.

[44] Ramalingam, C. and Mohan, P., 2021. Addressing semantics standards for cloud portability and interoperability in multi cloud environment. *Symmetry*, *13*(2), p.317.

[45] Ravi, N. and Thangarathinam, M., 2019. Emergence of Middleware to Mitigate the Challenges of Multi-Cloud Solutions onto Mobile Devices. *International Journal of Cooperative Information Systems*, *28*(04), p.1950012.

[46] Reddy, A.R.P. and Ayyadapu, A.K.R., 2021. Securing Multi-Cloud Environments with AI And Machine Learning Techniques. *Chelonian Research Foundation*, *16*(2), pp.01-12.

[47] Reinartz, W., Wiegand, N. and Imschloss, M., 2019. The impact of digital transformation on the retailing value chain. *International Journal of Research in Marketing*, *36*(3), pp.350-366.

[48] Rishu, V.K. and Sinha, S.A., 2021. Advancements in encryption techniques for enhanced data security over cloud. *Journal of Cybersecurity and Information Management*, *8*(2), pp.51-59.

[49] Sharma, H., 2020. Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on interoperability and comprehensive visibility. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), pp.1-18.

[50] Singu, S.K., 2021. Real-Time Data Integration: Tools, Techniques, and Best Practices. *ESP Journal of Engineering & Technology Advancements*, *1*(1), pp.158-172.

[51] Sivathapandi, P., Soundarapandiyan, R. and Krishnamoorthy, G., 2021. Platform Engineering for Multi-Cloud Enterprise Architectures: Design Patterns and Best Practices. *Australian Journal of Machine Learning Research & Applications*, *1*(1), pp.132-183.

[52] Surianarayanan, C., Chelliah, P.R., Surianarayanan, C. and Chelliah, P.R., 2019. Basics of Cloud Management. *Essentials of Cloud Computing: A Holistic Perspective*, pp.255-266.

[53] Tahirkheli, A.I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N. and Kim, K.I., 2021. A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. *Electronics*, *10*(15), p.1811.

[54] Tomarchio, O., Calcaterra, D. and Modica, G.D., 2020. Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks. *Journal of Cloud Computing*, *9*(1), p.49.

[55] Tricomi, G., Merlino, G., Panarello, A. and Puliafito, A., 2020. Optimal selection techniques for Cloud service providers. *IEEE Access*, *8*, pp.203591-203618.

[56] Watada, J., Roy, A., Kadikar, R., Pham, H. and Xu, B., 2019. Emerging trends, techniques and open issues of containerization: A review. *IEEE Access*, *7*, pp.152443-152472.

[57] Barika, M., Garg, S., Zomaya, A.Y., Wang, L., Moorsel, A.V. and Ranjan, R., 2019. Orchestrating big data analysis workflows in the cloud: research challenges, survey, and future directions. *ACM Computing Surveys (CSUR)*, *52*(5), pp.1-41.

[58] Zhang, W.Z., Elgendy, I.A., Hammad, M., Iliyasu, A.M., Du, X., Guizani, M. and Abd El-Latif, A.A., 2020. Secure and optimized load balancing for multitier IoT and edge-cloud computing systems. *IEEE Internet of Things Journal*, *8*(10), pp.8119-8132.

[59] Akinrolabu, O., New, S. and Martin, A., 2019, June. Assessing the security risks of multicloud saas applications: A real-world case study. In *2019 6th IEEE international conference on cyber security and cloud computing (CSCloud)/2019 5th IEEE international conference on edge computing and scalable cloud (EdgeCom)* (pp. 81-88). IEEE.

[60] Dev, N.K., Shankar, R. and Qaiser, F.H., 2020. Industry 4.0 and circular economy: Operational excellence for sustainable reverse supply chain performance. *Resources, Conservation and Recycling*, *153*, p.104583.