American Journal of Smart Technology and Solutions (AJSTS)

ISSN: 2837-0295 (ONLINE)

VOLUME 5 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Smart Technology and Solutions (AJSTS)

Volume 5 Issue 1, Year 2026
ISSN: 2837-0295 (Online)
DOI: https://doi.org/10.54536/ajsts.v5i1.6523
https://journals.e-palli.com/home/index.php/ajsts

Design and Security Challenges of Multi-Cloud Architectures for Large Enterprises

Abdullah Mehboob[1*], Omer Mehboob[1], Gul Rauf[2], Ali Mehboob[1]

Article Information

Received: September 01, 2025

Accepted: December 2, 2025

Published: March 18, 2026

Keywords

Cloud Governance. CSPM, Enterprise cloud, IAM Federation, Multi-Cloud Architecture, Security Challenges, Zero Trust

ABSTRACT

Adoption of multi-cloud architectures has become a strategic transformation for large organizations that want to scale, achieve flexibility in operations and resilience in lean and heterogeneous clouds. Although there are benefits, the application of multi- clouds presents major design and security challenges, such as the distribution of workloads, interoperability, identity, protection of data, network vulnerabilities, and regulatory adherence. This conceptual review analyzes the design of a multi-cloud architecture and related security issues, summarizing findings from academic sources, industry reports, and cloud standards published between 2021 and 2025. The framework-based synthesis applied in the study is used to categorize architectural models such as vendor specific, broker based, federated and service mesh-based systems, such as compatibility of existing systems to adhere to the API, data synchronization, and governance strategies. The security challenges are examined along six important dimensions, which include identity and access management, data privacy, network security, compliance, visibility and incident response, and shared responsibility gaps. The solutions to consider include Cloud Security Posture Management (CSPM), Zero Trust Architecture, unified identity and policy management, centralized encryption, and advanced network security mechanisms evaluated in the review. The future research directions include monitoring with AI/ML enhancements, automated compliance checking, standardization of cross-cloud identities, single governance platforms, and multi-cloud resiliency architecture. This review offers valuable practical guidance to enterprises and places particular emphasis on future research needs by offering a synthesis of design principles, security issues, and mitigation strategies to help develop secure, scalable and interoperable multi-cloud environments in the future.

INTRODUCTION

Multi-cloud, defined as an organisation strategically adopting two (or more) public clouds, often in conjunction with private clouds or on-premise infrastructure, has become a popular enterprise strategy, no longer a niche engineering pattern. (Rittinghouse & Ransome, 2015) stated that historically, the idea of cloud computing can be traced to the earliest distributed-computing concepts in the 1990s, however, the term cloud was applied practically when scalable, pay-as-you-use services, initially provided by Amazon Web Services (EC2 and S3) in 2006, Google (primarily with the early App Engine offerings in 2008) and Microsoft (Azure, soon after this) started offering them as described by (Quadri, 2017). Such milestones made computing not a hardware-dependent hard spend, but rather a software-defined, on-demand computing service that could be stitched together between providers (Raut, 2022). As businesses grew up using the cloud, the single provider model of a lift-and-shift evolved into more complex constructions. The hybrid clouds, which combined the private and the public clouds and, progressively, the multi-cloud structures, which used the strengths of various vendors to provide redundancy, cost-efficiency, performance, regulatory considerations and prevention of vendor lock-in (Anh, 2024). This historical trend, beginning with initially virtualized hosting up to complete platform and AI service, is the reason why multi-cloud has ceased to be an exotic architecture and has become an operational necessity in complex organizations.

Massive companies are now using a multi-cloud scale, and its penetration is constantly recorded as very high in industry surveys. State of the Cloud reports by Flexera and a review of (Mei, 2023) indicate that 87% and 89% of organizations are now using multiple cloud providers, and that multi-cloud security and FinOps tools are spreading most of all into large enterprises. Patterns of spending reflect this change in strategy-Gartner predicted an increase in public cloud end-user spending (with the worldwide public cloud spending specified to be in hundreds of billions of dollars) and estimated that hybrid and multi-cloud systems would be used by the overwhelming majority of organizations as cloud ecosystems become diversified (Ponnusamy & Spanner, 2023). In practice, the proportion of enterprise workloads (more than half of enterprise workloads and SMB workloads in some reports) is currently running in the public clouds, although a minority (approximately one-fifth) of workloads have been repatriated back to on-premises environments. This explains why most organizations can no longer design workloads around the environment of a single provider. Simultaneously, the median enterprise cloud bill has increased as recent industry surveys indicate that, in addition to wider cloud migration, an increasing proportion of organizations now spend over 12 million dollars per year on public

[1]King Fahad University of Petroleum and Minerals, Saudi Arabia
[2]Allama Iqbal Open University AIOU, Pakistan
[*] Corresponding author's e-mail: AbdullahMehboob1@outlook.com

cloud services, which is due to newer cost drivers such as AI/ML workloads

The requirement to have a secure, scalable, and interoperable design in multi-cloud environments is the logical extension of the intended use that motivates the adoption of a multi-cloud environment. (Jor, 2025) explained that enterprises are seeking multi-cloud to become more resilient (no single vendor outage), to attain best-of-breed capability stacking (such as combining analytics services with a specific AI tool of a vendor), or to address regulatory demands (such as regional data residency). To realize these advantages, it is necessary to have cloud-native designs that are able to scale elastically, ensure uniform identity and policy enforcement across domains, and ensure APIs and data flows are interoperable (Emma, 2024). Except carefully designed, the fragmentation that multi-cloud brings about can negate the benefits it is supposed to offer, blocks in performance, expensive replication of tooling and expertise, lack of uniform governance and fragile integration points that fail on demand or at attack (Bieger, 2023). Concisely, multi-cloud requires an architecturally clear networking, identity, data management, observability solution that is clearly designed for distributed heterogeneity, as opposed to an ad hoc solution.

Multi-cloud causes unique security and operational issues that are increasingly becoming urgent with the extent of use of cloud use. Polls of security vendors and customers indicate a minefield of inability to sustain strong security posture spanning a variety of providers. Microsoft's report on the State of Multi-Cloud Security and related industry surveys found that a significant portion of organizations cannot protect cloud-native applications and infrastructure through the development-to-runtime lifecycle (Rahman, 2025). An average of about 65% of code repositories had source-code vulnerabilities at least one time in at least one year, and those vulnerabilities took an average of close to two months (Iannone *et al.*, 2022). According to Talwar (2024), multiple organizations face misconfigurations, uneven logging, and struggle to manage encryption keys and identity policy across the clouds. These facts provide a problem statement to this review as big business organizations move to multi-cloud to achieve agility and resilience, they are met with a growing complexity in architecture and a disjointed security posture, combined to increase operational risk, compliance burden, and overall cost of ownership (Essien *et al.*, 2021). Therefore, the multi-cloud changes complexity from one platform to the inter-platform space, increasing the attack surface and magnifying governance vectors unless countered through integrative design and tooling.

In the light of such trends and pressures, this review presents specific research objectives and questions that will aim to synthesize the literature and industry evidence to present it to a practitioner and academic audience. It aims to (1) map the technical and historical history of multi-cloud architecture and the reasons why multi-cloud has become the dominant enterprise model; (2) list the most critical design issues, including networking, identity and access management (IAM), data consistency, observability, cost control, and workload placement, to create secure, scalable multi-cloud systems; (3) compare the security challenges that are unique or exaggerated in multi-cloud environments, such as cross-provider policy enforcement, key-management fragmentation, telemetry and incident-response gaps, and cross-jurisdictions compliance. The following are the research questions used to operationalize these objectives: What architectural patterns minimize the complexity of multi-cloud and maintain provider flexibility? What modifications must identity and data-control models undergo to maintain confidentiality and compliance across vendors? What monitoring and automation strategies prove to be effective in detecting and remediating incidents in a multi-cloud environment? And lastly, where do we have the gaps where future research and definitions work are most needed? These questions are selected to be both descriptive (what is happening) and prescriptive (what should be done), in keeping with the dual audience of researchers and enterprise.

This review has three contributions. Initially, it brings together the various empirical studies done in the industry, vendor risk reports, and academic literature into one narrative that connects the historical evolution, adoption rates, and technical design decision making, as such, offering a single source on why multi-cloud is now the centre of enterprise IT. Moreover, this review transforms issues of security into a practical taxonomy that makes responsibility apparent (provider versus enterprise) and risk can be limited through integrative design; the taxonomy is meant to assist architects in ranking investments in controls, automation and governance. Additionally, this review points to concrete research and standards gaps, such as the necessity of cross-cloud identity federations which scale safely, a standardized telemetry schema for multi-cloud observability and automated compliance verification tools which would, were they to be filled, materially lower operational friction and risk in large organizations.

LITERATURE REVIEW

Conceptual Foundations

To comprehend the conceptual foundation of multi-cloud environments, it is important to discuss the models of cloud deployment, the architectural grounds underlining the multi-cloud strategies, and the industry standards and frameworks that condition their practice. Those theoretical foundations are useful to highlight the major differences between cloud configurations and to provide insights into why large businesses are increasingly moving in the direction of multi-cloud as a strategic and safety-focused option. The positioning of multi-cloud in existing cloud theories, models, and frameworks presented in this section forms the foundation of the further analysis of design considerations and challenges

in terms of security.

Cloud Deployment Models

The theoretical foundation of the current literature on cloud deployment models has four prevalent models of public, private, hybrid, and multi-cloud models, which involve various forms of ownership, control, and responsibility of operation.

(Thallam, 2023), the public cloud model is defined by the common infrastructure, which is possessed and controlled by third parties (AWS, Azure, and Google Cloud). It is designed on a utility-based consumption model that is virtually unlimited in terms of scalability, global availability, as well as controlled services that reduce overheads in operations. Existing businesses have been using public cloud to support elastic workloads, analytics environments, or a global user-facing application. However, the public cloud presents the sharing of tenancy and the lack of direct control, and organizations should respond to this fact with the help of governance policies and technical controls (Mathur, 2024).

(Deb & Choudhury, 2021), the private cloud model provides dedicated infrastructure, which can either be on-premise or a private environment controlled by a provider. It is configured to suit organisations that need data locality, regulation or a very high degree of customization rather than configuration and security. Privately operated clouds, which may be based on VMware, OpenStack, or vendor-specific systems, offer additional control, however, their scalability and flexibility are restricted compared to public clouds (Vallabhaneni, 2021). The cost model is also more consistent with the traditional capital-intensive IT infrastructure because of the hardware acquisition and maintenance (Oladosu *et al*., 2021).

The hybrid cloud integrates the public and the private clouds into one operational architecture and allows the movement of workloads between the environments as required. This model offers a trade-off between scalability and control. Sensitive or controlled data can be stored on a private infrastructure, and burst workloads or customer-facing applications can utilize the elasticity of a public cloud. The hybrid cloud theories focus on the interoperability, secure connectivity (e.g., VPN, direct connect services) and standardized platforms in which heterogeneous resources can be managed (Ogbuefi *et al*., 2023). Practically, hybrid models can be used as a transition period by most companies that are moving off their legacy systems to cloud-native models.

However, multi-cloud is the active use of more than one provider of publicly available cloud services, frequently in combination with elements of a private cloud, in order to achieve better outcomes, diversify service provider capabilities, escape lock-in and enhance resilience (Merseedi & Zeebaree, 2024). Multi-cloud focuses on choice, redundancy and specialization, unlike hybrid cloud, which focuses on integrating between the private and the public clouds. The most critical enterprise-level factors are that there should be interoperability among provider APIs, identity and access management, cross-cloud governance, cost optimization and unified observability. (Shrivastava & Agrawal, 2024) stated that multi-cloud needs a more architectural solution since it will incur heterogeneity between providers, each having different service models, security implementations, networking constructs and operational paradigms. The complexity comes at the cost of the benefits that are high availability and global distribution, and regulatory agility, which are needed in organizations.

The Foundations of Multi-Cloud Architecture

Multi-cloud architecture is based on a layered cloud service model, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and deploys these services through a number of providers.

IaaS-based multi-clouds

IaaS-based multi-clouds have enterprises that use virtual machines, storage and networking hardware that are provided by other vendors. The model is popular in those organizations that desire to have maximum control over the workloads, besides minimizing dependence on any single vendor (Mehfuz, 2022). However, variations in virtual machine images, networking constructs and load balancing mechanisms demand a regular automated layer of infrastructure, typically executed with tools like Terraform, Kubernetes, or cross-cloud orchestrators.

PaaS multi-cloud

PaaS multi-cloud Organizations in PaaS-based multi-cloud use the services of various providers in managed databases, AI/ML platforms, application runtimes, or serverless environments. The architectural problem in this case will be to integrate incompatible proprietary services, such as the incorporation of Google Cloud's BigQuery analytics with AWS Lambda functions or Azure Machine Learning Studio (Imran *et al*., 2020). The abstractions found at the PaaS level provide the greatest benefits of an innovation but also the most specialization of the vendors, which requires careful planning of the architecture.

SaaS-integrated multi-cloud

Under SaaS-integrated multi-cloud, businesses integrate cloud-based applications, including CRM systems, ERP solutions and communication suites that need to communicate with workloads that may be operating in a number of other cloud environments. In SaaS-focused multi-cloud, API management, secure identity federation and platform-to-platform data synchronization are placed in the spotlight (Gajwani, 2025). The strategies based on multi-cloud workload distribution are based on optimization theory. The following are some of the distribution patterns that are often used by enterprises:

• Workload specialization - workloads are assigned to a provider that is best at a given specific service (e.g. AI workloads to Google Cloud, enterprise authentication

workloads to Azure).

• Redundancy-based allocation - It is the deployment of redundant instances of the same system on the clouds to provide a failover and continuity.

• Geographic optimization - choosing providers that are the most geographically compliant in terms of latency or data residency.

• Cost-based allocation - involves the application of pricing models, spot incidences, or discounts to lower operational costs.

• Risk diversification - reducing the risks of outages, legal constraints or even vendor transitions, by verifying that workloads are not limited to a single provider.

Standards and Frameworks

Multi-cloud has operational and security foundations that are governed by standards and frameworks that determine the way organizations design, deploy, and manage distributed systems. Another conceptualization of a cloud system that is among the most authoritative is the NIST Cloud Computing Framework. According to Wijaya (2022)(Wijaya & Avian, 2022), NIST introduces the features that are characteristic of clouds (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), and it separates service and deployment models and defines the following roles, cloud service providers, consumers, auditors, brokers, and carriers. In the case of multi-cloud, NIST is important because it provides a standard vocabulary and architecture base that can be used to ensure organizations are able to combine several providers uniformly (Bieger, 2023). Security evaluations, compliance evaluations, and architectural documentation of multi-cloud environments are commonly guided by the NIST structure.

Zero Trust Architecture (ZTA) has emerged as a paradigm of security in multi-cloud at a faster rate. It does not support the concept of implicit trusting on the basis of network location but rather demands constant validation of identities, devices, and workloads (Fernandez & Brazhuk, 2024). The classical model of security can not be applied in multi-cloud setups where workloads cut across several perimeters and networks. The principles that are presented by ZTA include least privilege, micro-segmentation, secure identity enforcement, and real-time monitoring of distributed systems. When implemented on multi-cloud, Zero Trust allows the identity and policy enforcement to be consistent even when workloads are transferred between providers (Phiayura & Teerakanok, 2023). This helps to decrease cross-cloud breaches, reduce the lateral movement and enhance the overall governance.

Another theoretical point of constructing the multi-cloud security is the Shared Responsibility Model, which was first formulated by cloud providers. The model separates responsibilities of the provider (who is tasked with ensuring infrastructure security) and the customer (who is tasked with ensuring applications, data, and access security). But in multi-cloud, this model is more complicated, because of differences in provider policy, service-level agreement and security controls. Firms should thus develop a single, cross-cloud security governance framework that takes into consideration the disparity in identity mechanisms, logging functions, encryption alternatives and compliance certifications. Theoretical applicability of the shared responsibility model to multi-cloud is that it serves as a risk allocation and control implementation structure and audit preparedness guide applied in heterogeneous environments.

MATERIALS AND METHODS

A conceptual review methodology is used in this study, which is suitable to summarize theoretical knowledge, architectural models, and security frameworks concerning multi-cloud environments. The review was based on the analysis, interpretation, and synthesis of the current academic and industry literature aimed at developing a detailed picture of the design and security issues relevant to multi-cloud architectures within large corporations. The conceptual review method enables the study to cover various opinions in the field of cloud engineering, cybersecurity, distributed systems, and enterprise computing, therefore, allowing for an assessment of the issue holistically.

In order to achieve academic rigor, a structured search strategy was applied on major digital libraries such as IEEE Xplore, Scopus, SpringerLink, ACM Digital Library and Google Scholar. These databases have been chosen as they encompass peer-reviewed articles, conference proceedings, technical standards, and other authoritative books on cloud computing. The search strategy was used on a combination of primary and secondary keywords and Boolean operators, and filters of publication year. The list of databases and the selected search strategies to find the corresponding literature is provided in Table 1.

Table 1: Search Strategy and Databases Used

Database	Search Strings / Keywords Used
IEEE Xplore	"multi-cloud security" OR "multi-cloud architecture" AND "enterprise cloud"
Scopus	"Cloud architecture design", "multi-cloud interoperability", "distributed cloud security"
SpringerLink	"Hybrid and multi-cloud", "zero trust cloud", "multi-cloud governance"
ACM Digital Library	"Cloud workload distribution", "cloud security frameworks", "cross-cloud identity management"
Google Scholar	"multi-cloud computing challenges", "shared responsibility model", "cloud standards NIST"

The search process was conducted with the help of a set of carefully selected keywords, such as: multi-cloud security, cloud architecture, multi-cloud interoperability, enterprise cloud adoption, zero trust architecture, cloud governance, shared responsibility model, distributed cloud systems, and multi-cloud design patterns. These search terms were based on the research objectives and coverage of technical, architectural, and security topics. Studies were then screened against pre-defined inclusion and exclusion criteria after having first obtained initial results to be relevant and of academic quality. Peer-reviewed journal articles, conference papers, and cloud standards frameworks were considered in the review. The studies included were published from 2016 to 2025 only to reflect the most recent changes, as multi-cloud structures and related security frameworks have evolved at a rapid pace over the last ten years. The criteria are summarized in Table 2.

Table 2: Inclusion and Exclusion Criteria

Criteria Type	Description
Inclusion Criteria	Studies published between 2021–2025; peer-reviewed; focused on multi-cloud architectures or security; relevant to enterprise adoption; English language; includes theoretical, technical, or architectural analysis.
Exclusion Criteria	Studies before 2021; non-academic blogs; vendor promotional material; studies focused only on single-cloud environments; duplicates; papers without full text available.

RESULTS AND DISCUSSION

Multi-Cloud Architecture Design for Large Enterprises

Multi-cloud architectures are rapidly becoming increasingly popular with large enterprises in an effort to enhance resilience, minimize vendor lock-in, and optimize workload placement. Gartner (2023) states that in the world, 76% of businesses today have more than two cloud providers, up from 52 in 2019 as highlighted by (Ediga, 2025). There are four significant paradigms of architecture prevailing. Multi-cloud solutions that are vendor-specific use proprietary solutions provided by hyperscale's such as AWS Outposts, Azure Arc or Google Anthos. Such models are easy to deploy, but can recreate indirect risks of lock-in since enterprises rely on the orchestration logic and the API structure of each provider (Peiris *et al*., 2021). However, vendor-specific solutions are still appealing to organizations that assume compliance as a priority, and AWS claims that configuration overhead has decreased by 34 % in cases of native extensions to the multi-clouds.

The architectures of brokers work with the help of an automated system known as a cloud broker that manages the provisioning of the resources, cost control, and performance measurements among a set of providers (Khan *et al*., 2024). Broker-based systems offer single dashboards of management and automatic schedules of workloads, and in large-scale implementations, can reduce the complexity of operation by up to 18-23%. Nevertheless, brokers create an extra control level, and it can become a bottleneck when the workloads are at their highest (Ospina Herrera, 2024). According to (Tricomi, 2021), federated cloud systems are more decentralized the providers are interoperable by sharing common standards, usually based on the Open Cloud Computing Interface (OCCI). The federated models are especially applicable in organizations where data locality requirements are high, like in healthcare or financial institutions. According to recent research (Austin, 2024), federated designs can enhance cross-cloud portability by 40%, but interoperability issues remain. The multi-cloud networking (facilitated by tools such as Istio or Linkerd) based on service-mesh has become a very scalable data architecture.

Enterprise Integration Reconsiderations

Enterprises with large businesses have a big problem with integration because the multi-cloud systems need to coexist with infrastructure that could be decades old. Integration of legacy systems is also one of the longest-lasting barriers, and estimates that more than 60% of enterprise applications have legacy elements that cannot be integrated with cloud-native systems. (Kansara, 2021) explained that multi-cloud migration thus demands the use of abstraction layers by middleware or containerization policies that allow the reuse of the ageing workloads in a variety of cloud environments without massive re-engineering. Another important dimension is API management and interoperability. Multi-clouds are more likely to make use of mixed API formats, authentication systems and event message patterns. In the absence of powerful API gateways or federated API regulation, failures in interoperability can decrease the performance of distributed workflows by 15.20% (Rahaman, 2025). Businesses then use cohesive platforms of API management (such as Kong, Apigee) to streamline REST, gRPC and GraphQL interactions across clouds.

Data consistency and synchronization are always important in the operations of the multi-cloud, and especially in cases where the transactional systems that are of high volume are distributed across geographical boundaries. (Oloruntoba, 2025) literature studies indicate that the variation in cross-cloud replication can lead to a difference in data by up to 8 milliseconds per write cycle, with financial and real-time analytics being the most affected industries. Distributed consensus protocols (e.g., Raft, Paxos), event-sourcing patterns,

and conflict-free replicated data types (CRDTs) are some of the techniques used to preserve consistency without jeopardizing throughput. The centralized and decentralized governance systems shape the general model of control in the multi-cloud adoption of an enterprise. Centralized Governance-this is the most favored by organizations that have high compliance requirements, it provides consistency in security control, identity management and policy enforcement (Ghadge, 2024). However, decentralized governance has more flexibility, allowing domain-driven groups to maximize the workloads per cloud provider.

Factors of Performance and Scalability Design

The optimization of performance is an overriding goal of multi-cloud architecture. The most important determinants of system reliability are latency, scheduling of the workload, and load balancing. The cross-cloud traffic may add latency of 40-80 ms based on the geographical distance and the provider's infrastructure (William & Richard, 2025). To address this, businesses use latency-sensitive load balancers, global traffic controllers, and AI-driven workload schedulers that dynamically redirect requests to the nearest-latency cloud endpoint. Multi-cloud deployments should also take into consideration the distributed computing facts like data partitioning, edge offloading and cross-provider bandwidth constraints. According to the studies, high-frequency workloads can have up to 45% of compute overhead reduced by edge-cloud synergy (Rahman, 2025). Correspondingly, distributed microservice systems demand close coordination to prevent ripple effects in case of network overload.

The strategies of resource optimization, such as autoscaling, predictive demand modelling, container bin-packing and the use of spot-instances, are important in the maintenance of cost and performance efficiency (Ghafouri, 2024). According to the internal benchmarks of Google Cloud (2021), with predictive autoscaling, the costs of compute can be reduced by 17-24%, and the response time remains stable even when traffic increases unexpectedly (Chen *et al.*, 2025). Multi-cloud cost governance platforms also assist organizations in analyzing their spending pattern, predicting peak demands, and avoiding excessive provisioning of resources.

Multi-Cloud Security Challenges

Identity and Access Management (IAM) Complexity

Multi-cloud Identity and Access Management (IAM) is a highly complex task because it allows vendors to choose the vendor, which has its own authentication, privilege models, and policy settings. Authentication with multiple vendors can easily introduce a non-uniform system regarding the handling of credentials and require employees to have different identities in AWS, Azure, and Google Cloud (Memis, 2023). Microsoft (2024) suggests that 61 % of enterprises indicated having at least one occurrence of improperly configured IAM policies that resulted in momentary privilege growth (Xu *et al.*, 2024). In federated systems, the cross-cloud privilege escalation is especially worrying as the misaligned roles may spread the permissions to many platforms. Widely-recommended solutions include single sign-on (SSO), multi-factor authentication (MFA), as well as federated identity protocols (Aldea & Bocu, 2025).

Data Protection and Confidentiality Issues

The issues of data security and privacy are very important with multi-cloud architecture. Data fragmentation is where sensitive information is shared with multiple providers, who receive data on different jurisdictions. A 2023 survey reported a figure of 47% of enterprises that expressed worries about compliance because of the data sovereignty issue (Yun, 2025). Managing the keys in a multi-cloud storage or usage system is much more complicated than when the key is held or employed in a single cloud. Breach or loss of access can be a result of mismanagement.

Network Security Issues

Multi-cloud networking creates additional routing, segmentation and traffic control vulnerabilities. Critical workloads can be exposed to misconfigured virtual networks, over-permeable security groups, or incorrect firewall rules. The shared responsibility model usually makes it hard to establish the responsibilities of network protection between customers and providers. Another issue is distributed Denial-of-Service (DDoS) vectors; according to the research provided by (Hoque *et al.*, 2025), multi-cloud enterprises are 25 times more prone to cross-provider DDoS propagation because of insufficient inter-cloud filtering. Service-mesh and encrypted inter-service communication solutions reduce certain risks but increase the complexity of operations.

Regulatory and Compliance Issues

Compliance with regulations in multi-clouds is challenging in nature. Regulations like GDPR, HIPAA, ISO 27001, and PCI-DSS present rigorous demands in data processing, storage, and auditing. However, it may be tricky to demonstrate compliance with various providers in most cases because of discontinuous logs, varied reporting templates, and regional certifications (Ahuja, 2024). According to records that more than half of big companies noted problems with proving compliance with regulations in relation to multi-cloud systems, which may result in fines, damaged reputation, or contractual fines (Sivaseelan, 2024).

Visibility, Monitoring and Incident Response

Interoperability among distributed clouds is not always visible. Pieced together, logging and telemetry provide loopholes that inhibit threat detection. Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools are utilized by many enterprises, but the problem of

integration between various providers is still a challenge (Rathore, 2024). According to the report conducted by IBM in 2024, multi-cloud organizations reported waiting as long as 62% to respond to an incident because of poor coordination in monitoring and fragmented mechanisms of sending alerts. Cross-cloud dashboards and unified observability platforms are becoming available, as their usage remains low because of technical complexity and cost.

Shared Responsibility Model Gaps

The shared responsibility model, which forms the basis of cloud security, tends to confuse a multi-cloud environment. Businesses can be confused about the provider that offers infrastructure security and data and application protection. Incoherent practices among providers may pose a loophole that attackers can use. According to Cloud Security Alliance (2023), about 29% of multi-cloud breaches were caused by failures because of shared responsibility assumptions. These risks would be mitigated through clear documentation, provider alignment, and central governance structures.

Current Security Solutions and Best Practice

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) software offers real-time visibility of multi-clouds to identify misconfigurations, implement security policies, and minimize compliance loopholes. Prisma Cloud, DivvyCloud, and Trend Micro Cloud One are among the CSPM solutions that enable organizations to detect over 70% of typical misconfigurations open storage buckets, exposed APIs, and unnecessary IAM privileges (Gartner, 2023). Trends in enterprise adoption indicate that an estimated 62 % of large enterprises have now adopted CSPM solutions to manage multi-cloud security, a significant increase on the 38 % in 2018. CSPM tools have weaknesses despite their advantages. They are mostly used to deal with configuration drift and compliance, but they do not defend against a high-level threat, like a zero-day vulnerability or insider attack. Moreover, the implementation of CSPM results in central security activities must be orchestrated to prevent the risk of alert fatigue between various cloud providers.

Zero Trust in Multi-Cloud Architecture

Zero Trust Architecture (ZTA) has become a foundation of multi-cloud protection through the enforcement of the principle of never trust, always verify. Multi-cloud implementation of ZTA encompasses micro-segmentation to separate workloads and keep them from moving laterally, and regular checking of user and device identities (NIST, 2020). Micro-segmentation will mean that even in case one cloud workload is breached, other resources will not be exposed to an attacker at will, and the effects of breaches will be greatly mitigated. Those organizations which have implemented the principles of Zero Trust have seen a 33% decrease in lateral movement concerning breaches. Multi-clouds support multi-cloud environments, ZTA expects to perform identity verification and policy enforcement in a heterogeneous provider environment. A combination of service meshes and automated policy enforcement tools with the rising popularity of Kubernetes and containerized microservices has rendered ZTA especially effective.

Unified Identity and Policy Management

The identity management of a multi-cloud environment is often disjointed and thus prone to misconfigurations and escalation of privileges. IAM federation is a solution to this problem because it enables a centralized verification of identities across multiple cloud providers, thus enabling enterprises to use Single Sign-On (SSO), Multi-Factor Authentication (MFA), and role-based access controls in a standardized manner. Microsoft (2024) advises enterprises that adopted federated IAM to reduce incidents related to access by 40% since its adoption. Additional to IAM federation, policy-as-code tools, including Open Policy Agent (OPA), Terraform and Pulumi, enable enterprises to express and implement security and compliance policies programmatically. The tools make it possible to deploy policies on a variety of clouds in a version-controlled and automated way that minimizes the risk of human errors and enhances governance in an efficient way. Best practices propose that when implementing IAM federation, policy-as-code frameworks are also used to provide consistent, auditable, and enforceable access control in heterogeneous environments.

Key Management and Encryption

The security of sensitive data in multi-clouds is vital with respect to the encryption and key management. Businesses are moving towards centralized key management systems, including cloud-native Key Management Systems (KMS) or Hardware Security Modules (HSM), to ensure uniform policy of encryption across clouds. Managing KMS fragmentedly has many risks: centralized KMS ensures the rotation, auditing, and control of keys, and it reduces risks (Cloud Security Alliance, 2023). The best practices of cross-cloud encryption are end-to-end encryption of data in transit and at rest, key storage on hardware, and the application of standard encryption protocols like AES-256 and TLS 1.3. The research has shown that companies that embrace the idea of integrating key management and standardized encryption minimise the chances of instances of data exposure by 28% (PwC, 2023).

Network Security Improvements

A secure service mesh, API gateway and distributed firewalls can be combined to enhance network security in multi-cloud architectures. Service meshes such as Istio or Linkerd also offer service-to-service encrypted communications, traffic routing policies and fine-grained access control, which are critical in containerized workloads across multiple providers. The API gateways

make cross-cloud attacks inaccessible to microservices by verifying authentication, rate limiting, and detecting threats at the application layer. Besides, distributed firewalls enable businesses to use uniform network policies on heterogeneous clouds. (Gartner, 2025) notes that institutions with integrated network protection, regardless of the cloud, note a reduction in network-related attacks, up to 22 %. Best practices such as integrating centralized policy orchestration with real-time telemetry can be used to identify and prevent anomalies quickly in all cloud environments. Therefore, to achieve multi-cloud configurations in large corporations, layered and integrated solutions integrating automated configuration management (CSPM), Zero Trust principles, federated identity, and policy-as-code, centralized encryption, and overall network controls are necessary. Implementation of these best practices can decrease the chances of breaches also guarantee regulatory compliance, operational efficiency and resistance to changing threats. Multi-Cloud security can be most efficient when applied as a complex system instead of a set of uncoordinated tools and operations.

Future Research Directions

Although the use of multi-cloud architectures has been increasing, there are a number of research gaps that have restricted the potential of massive enterprise implementations. The necessity of standard multi-cloud governance platforms is one of them. In many cases, the current solutions are independent to each provider on how to enforce the policies, audit them and view them and as a result, policy enforcement, auditing and visibility are fragmented. It is recommended that the future studies examine the frameworks that would combine governance of heterogeneous clouds but be compliant, cost-efficient and operationally agile. Another significant direction is the automated compliance verification. In a multi-geography environment with regulations like GDPR, HIPAA and PCI-DSS, compliance verification in a distributed environment is not only time-consuming, but also prone to error. Studies on AI-based compliance technology to automatically verify configuration, access control and data residency can minimize manual audits and increase the level of assurance. Multi-cloud monitoring with AI and machine learning is a potential future. Anticipatory detection of anomalies, intelligent workload placement, and proactive response to threats would help prevent the performance bottlenecks and security breaches before they compromise the operations. Initial investigations imply that AI has the potential to cut the time of incident detection by 40% (IBM, 2023), yet additional research is required in this area to overcome cross-cloud integration issues. Moreover, cross-cloud identity structures should be standardized to make IAM federation, SSO and enforcement of policies easier. Studies must be done on developing vendor-neutral identity and access standards that can be used in authentication without compromising security. Lastly, less research has been conducted on the topic of multi-cloud resiliency and disaster recovery models, such as active-active deployments, geo-redundancy, and failover orchestration. The studies in the field can assist companies to secure business continuity at the lowest possible cost and compliance levels in multi-cloud ecosystems.

CONCLUSION

The present review identifies the basic design concerns and security issues to multi-clouds in the enterprise-scale. The adoption of multi-clouds allows scalability, redundancy, and optimalization of workload, yet it demands thorough choice of architecture models, such as vendor-specific, broker-based, federated, and service-mesh-based. Integration of enterprises requires consideration of compatibility of legacy systems, API interoperability, data synchronization and balanced governance policies. Latency-conscious scheduling, distributed computing, and resource optimization systems ensure the sustainability of service quality and performance and scalability. Multi-cloud environments on the security front present complex IAM management, data privacy issues, network vulnerability, regulatory compliance problems, visibility, and shared responsibility ambiguity. These need to be addressed with layered security practices, such as Cloud Security Posture Management (CSPM), Zero Trust Architecture, federated IAM with policy-as-code, and centralized encryption and key management, as well as with a robust network security control, like service mesh and distributed firewalls. The review emphasizes the significance of cohesive, uniform multi-cloud security structures, which balances efficiency in operation, compliance, and risk reduction. It is suggested that enterprises should embrace a singular governance framework, deploy perpetual surveillance, concretize policies, and create solid disaster recovery designs. The research directions of the future are automation, AI/ML integration, standardization of cross-cloud identity, and resiliency models with greater strength. Through such aspects, multi-cloud architectures will be able to realize their potential and provide secure, scalable, and interoperable approaches to support the ever-changing needs of large organizations.

REFERENCES

Aldea, C. L., & Bocu, R. (2025). Authentication Challenges and Solutions in Microservice Architectures. *Applied Sciences, 15*(22), 12088.

Anh, N. H. (2024). Hybrid Cloud Migration Strategies: Balancing Flexibility, Security, and Cost in a Multi-Cloud Environment. *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems, 14*(10), 14–26.

Austin, M. (2024). Multi-cloud Strategies and Interoperability Issues.

Bieger, V. (2023). A decision support framework for multi-cloud service composition

Chen, J., He, X., Ye, H., Jiang, F., Zhang, T., Chen, J., &

Gao, X. (2025). Online Ensemble Transformer for Accurate Cloud Workload Forecasting in Predictive Auto-Scaling. arXiv preprint arXiv:2508.12773.

Deb, M., & Choudhury, A. (2021). Hybrid cloud: A new paradigm in cloud computing. Machine learning techniques and analytics for cloud security, 1–23.

Ediga, R. (2025). Enabling Unified Digital Experiences at Scale: The Strategic Role of Cloud Platforms in Modern Digital Experience Architecture. *Journal Of Engineering And Computer Sciences, 4*(6), 173–180.

Emma, O. (2024). An Analysis of Multi-Cloud Implementation Strategies and Their Impact on Disaster Recovery: Building Resilience and Excellence in Enterprise Computing.

Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2021). Secure configuration baseline and vulnerability management protocol for multi-cloud environments in regulated sectors. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(3), 686–696.

Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces, 89,* 103832.

Gajwani, G. A. (2025). Microservices Architecture for Loan Trading Platforms: A Digital Transformation Approach.

Gartner, G. (2025). A decade in scientific cartography: insights and future directions. *International Journal of Cartography, 11*(2), 166–172.

Ghadge, N. (2024). Enhancing Identity Management: Best Practices for Governance and Administration. *Computer Science & Information Technology* (CS & IT), 219–228.

Ghafouri, S. (2024). Machine Learning in Container Orchestration Systems: Applications and Deployment Queen Mary, University of London].

Hoque, S., Aydeger, A., Zeydan, E., & Liyanage, M. (2025). A Survey on Distributed Denial of Service Attack Mitigation for 5G and Beyond. *IEEE Open Journal of the Communications Society.*

Iannone, E., Guadagni, R., Ferrucci, F., De Lucia, A., & Palomba, F. (2022). The secret life of software vulnerabilities: A large-scale empirical study. *IEEE Transactions on Software Engineering, 49*(1), 44–63.

Imran, H. A., Latif, U., Ikram, A. A., Ehsan, M., Ikram, A. J., Khan, W. A., & Wazir, S. (2020). Multi-cloud: a comprehensive review. 2020 ieee 23rd international multitopic conference (inmic),

Jor, N. (2025). Evaluating the Effectiveness of Multi-Cloud Strategies in Enhancing Enterprise Agility and Scalability.

Kansara, M. (2021). Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. *International Journal of Applied Machine Learning and Computational Intelligence, 11*(12), 78–121.

Khan, M. H., Habaebi, M. H., & Islam, M. R. (2024). A systematic literature review of cloud brokers for autonomic service distribution. IEEE Access.

Mathur, P. (2024). Cloud computing infrastructure, platforms, and software for scientific research. High Performance Computing in Biomimetics: *Modeling, Architecture and Applications,* 89–127.

Mehfuz, A. J. K. S. (2022). CLOUD USAGE AUTHENTICATION SCENARIOS BASED API ACCESS. *Advance and Innovative Research, 368*.

Mei, L. (2023). Cost Optimization in cloud costs with FinOps and multi-cloud billing monitoring tool.

Memis, F. E. (2023). Identity Lifecycle Management in Cloud Service Providers.

Merseedi, K. J., & Zeebaree, S. R. (2024). The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment. *The Indonesian Journal of Computer Science, 13*(2).

Ogbuefi, E., Ogeawuchi, J. C., Ubamadu, B. C., Agboola, O. A., & Akpe, O. (2023). Systematic review of integration techniques in hybrid cloud infrastructure projects. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 1634–1643.

Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. *Magna Scientia Advanced Research and Reviews, 2*(1).

Oloruntoba, O. (2025). Architecting Resilient Multi-Cloud Database Systems: Distributed Ledger Technology, Fault Tolerance, and Cross-Platform Synchronization. *International Journal of Research Publication and Reviews, 6*(2), 2358–2376.

Ospina Herrera, J. P. (2024). Architecture for distributed systems that facilitates a cloud-native AIOps implementations.

Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks. John Wiley & Sons.

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. *Ieee Access, 11,* 19487–19511.

Ponnusamy, A., & Spanner, A. (2023). Technology Operating Models for Cloud and Edge: Create your purpose-built distributed operating model for public, hybrid, multicloud, and edge. Packt Publishing Ltd.

Quadri, S. (2017). Cloud computing: migrating to the cloud, Amazon Web Services and Google Cloud Platform S. Quadri].

Rahaman, M. M. (2025). The Role Of AI-Enabled Information Security Frameworks in Preventing Fraud In US Healthcare Billing Systems. ASRC Procedia: *Global Perspectives in Science and Scholarship, 1*(01), 1160–1201.

Rahman, R. (2025). Enhanced Security with Microsoft Defender for Cloud. In Pro Azure Governance and Security: A Comprehensive Guide to Safeguarding Your Cloud Computing (pp. 125–211). Springer.

Raut, K. R. (2022). The Concept of Cloud Computing and Its Security Issues.

Rittinghouse, J. W., & Ransome, J. F. (2015). Cloud Computing: History and Evolution. *Encyclopedia of Information Systems and Technology-Two Volume Set, 1,* 178–192.

Shrivastava, S., & Agrawal, Y. (2024). Multi-Cloud Deployments and Hybrid Cloud Architecture. In: Resmilitaris.

Sivaseelan, S. (2024). Enhancing Cyber Resilience in Multi-Cloud Environments. In.

Talwar, S. (2024). Unified Framework for Securing Cloud-Native Storage: Approach for Detecting and Mitigating Multi-Cloud Bucket Misconfigurations. In.

Thallam, N. S. T. (2023). Comparative Analysis of Public Cloud Providers for Big Data Analytics: AWS, Azure, and Google Cloud. *International Journal of AI, BigData, Computational and Management Studies, 4*(3), 18–29.

Tricomi, G. (2021). Study and evaluation of service-oriented approaches and techniques to manage and federate Cyber-Physical Systems.

Vallabhaneni, G. N. (2021). Comparison and Contrast of OpenStack and OpenShift.

Wijaya, G., & Avian, A. (2022). Analysis of cloud computing infrastructure system with nist standard cloud computing standards roadmap. CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences,

William, E., & Richard, T. (2025). Cross-Cloud Networking and Service Discovery Mechanisms.

Xu, J., Stokes, J. W., McDonald, G., Bai, X., Marshall, D., Wang, S., Swaminathan, A., & Li, Z. (2024). Autoattacker: A large language model guided system to implement automatic cyber-attacks. arXiv preprint arXiv:2403.01038.

Yun, H. (2025). China's data sovereignty and security: Implications for global digital borders and governance. *Chinese Political Science Review, 10*(2), 178–203.