International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT25111668

Automated Compliance Enforcement in Multi-Cloud Database Environments: A Comparative Study of Azure Purview, AWS Macie, and GCP DLP

Veeravenkata Maruthi Lakshmi Ganesh Nerella

Sr. Database Administrator, Summerfield, NC, USA

ARTICLEINFO

Article History:

Accepted : 21 June 2025

Published: 23 July 2025

Publication Issue

Volume 11, Issue 4

July-August-2025

Page Number

270-283

ABSTRACT

multi-cloud database compliance enforcement Automated compliance enforcement of databases accessed on multi-cloud platforms is needed to address changing regulatory requirements in dynamic cloud architecture. The lightning speed of the introduction of cloud computing has reshaped mode of data management and storage in organizations, making it more scalable, flexible, and cost-effective. But, with the growing application of multi-cloud infrastructures with more than one cloud service provider, including Amazon Web Services (AWS) and Microsoft Azure, and Google Cloud Platform (GCP), the action has brought about intricate issues regarding data compliance, regulatory conformity, and data security techniques. This paper will offer a detailed examination of data compliance in multi-cloud architecture along with the significant regulatory frameworks including GDPR and HIPAA, and the obstacles met during the structural integration and migration in multi-cloud. It also underlines the need to automate compliance to meet a changing regulatory environment and to mitigate the risk of operations. Additionally, the paper attributes AWS, Azure, and GCP along various fronts such as pricing, performance, security, usability, and data management to help organizations make superior decisions on their cloud adoption. Lastly, it draws roadmaps toward more compliance management with AI-based automation and blockchain-based audit, where future goals will focus on improving transparency and resiliency of the distributed cloud platforms.

Keywords—Cloud computing, data compliance, multi-cloud, GDPR, HIPAA, AWS, Microsoft Azure, GCP, cloud migration.

Introduction

The provision of computer resources, including databases, software, and resources, over the Internet that transcends local hardware is known as cloud computing. [1]. The paradigm allows firms to scale operations on demand, by delegating management of their infrastructure to commercial cloud service providers like AWS, Microsoft Azure and GCP [2][3]. In context of digital transformation rate, the more businesses incorporate cloud-based services, the more they businesses have optimize operations, augmented agility and become financially optimized.

Organizations increasingly use multi-cloud or hybrid multi-cloud strategies to achieve variety of technical and regulatory requirements [4]. They entail an integration of both on-premises infrastructure with utilization of public cloud services to gain flexibility of operation and business continuity. Nevertheless, these settings bring in dynamic challenges regarding compliance handling and security governance especially when dealing with sensitive data that is regulated in different frameworks [5]. Cloud security includes a system of tools and practices that are designed to reduce internal or external risks that would target cloud-based resources. During migration of workloads between heterogeneous cloud platforms it is important that security and compliance policies are consistently and audibly enforced in organizations. The verification of compliance in dynamic and multi-cloud environments is neither feasible nor scalable to be carried out manually.

Automated intelligent tools are used in order to ensure that compliance processes are maintained constantly across platforms. Reacting to this, large cloud providers have designed powerful, automated tools to deal with compliance and governance [6] [7]. Amazon Macie is a machine learning-based service that involves finding and protecting sensitive data offered by AWS. In Microsoft Azure, Purview offers an end-to-end data governance product that uses metadata, classifies data, and provides compliance expertise. The Data Loss Prevention (DLP) APIs offered by GCP allow finding sensitive data, identifying and anonymizing it on the fly at scale [8]. Although the multi-cloud model adds flexibility and innovation, it requires automated ways of monitoring and enforcement of compliance policies without interruption of services. This paper carries out a comparative analysis of the current Azure Purview, AWS Macie, and GCP DLP with regard to functionality, shortcomings, and applicability in the multi-cloud database environment. Comparatively, the Amazon Data Pipeline is a good mechanism that offers a flexible workflow orchestration in data movement and processing by integrating smoothly with AWS tools such as S3 and Redshift.

A. Structure of the Paper

The document is structured in following way: **Section II** discusses data compliance in multi-cloud environments. Section III An Overview of AWS, Microsoft Azure and GCP. Section IV renders a detailed study of comparative study of GCP, AWS and Microsoft Azure. Section V summarizes key findings from related research. Section VI concludes the paper and suggests future directions.

Data Compliance In Multi-Cloud Environments

Data adherence in cloud computing encompasses various components that organizations must consider to corroborate the secure and lawful handling of sensitive information as explained in Figure 1 [9]. With the increasing reliance on cloud technologies, compliance frameworks have evolved to address key aspects such as data privacy and protection, security and confidentiality, sovereignty and localization, and integrity and availability. These components form the backbone of a comprehensive data compliance strategy, allowing organizations to effectively mitigate risks while meeting regulatory obligations. Computer resources can be automatically collected, used, and managed using cloud computing, which is based on an internet-based platform. Cloud computing data centers offer colossal range of services to companies and consumers through tightly linked resources that may be added or deleted quickly and simply as needed. Depending on the cloud delivery model used, different sorts of services are offered. “SaaS”(Software as a Service), “IaaS” (Infrastructure as a Service), and “PaaS” (Platform as a Service) are three primary service models offered by cloud computing.

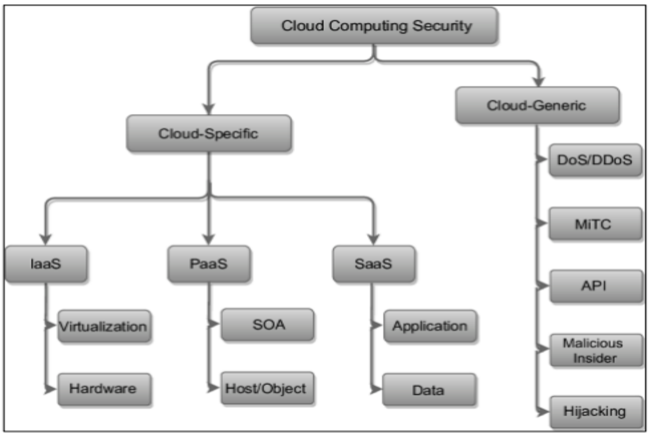

Figure 1. Taxonomy of Cloud Computing Security

A. Regulatory Requirements in Cloud Data Management (GDPR, HIPAA)

To protect the privacy and personal information of its residents, the European Union passed GDPR, a comprehensive data protection regulation. [10][11]. It has significant ramifications for every organization, regardless of location, that handles or keeps the personal information of people living in the EU. Due to the possibility of data being processed or kept in several countries, frequently across borders, cloud computing makes GDPR compliance more difficult.

A federal legislation in the United States called the Health Insurance Portability and Accountability Act (HIPAA) was created to safeguard the confidentiality and integrity of people's medical records. Cloud service providers that handle electronic Protected Health Information (ePHI) are frequently considered business associates of covered organizations, including health plans and healthcare providers, for the purposes of HIPAA.

B. Compliance Barriers in Multi-Cloud Architectures

Multi-cloud AI deployments must address complex regulatory requirements that exist among different jurisdictions because they present one of the major deployment challenges [12]. The governments of various nations enforce rigorous data protection regulations to determine where and under which conditions their data can be placed and utilized. Regulations such as:

- General Data Protection Regulation GDPR) – European Union
- California Consumer Privacy Act (CCPA) – United States
- Personal Data Protection Act (PDPA) – Singapore
- Data Security Law – China

Businesses must apply strict regulatory elements for data localization requirements alongside restrictions about international transfers and storage regulations. Multiple regional enterprises face complex challenges with AI model and cloud provider compliance because different regions have dissimilar legal opinions and these rules evolve over time.

C. Automating Compliance Across Cloud Platforms

The tremendous increase in cloud services has come with new forms of regulatory scrutiny to organizations as well as mounting compliance audit. The conventional compliance techniques are slow, expensive and may involve human error thus compromising chances of compliance and subsequent fines [13]. As an example, to stay compliant with ISO 27001 and PCI DSS, organizations are expected to keep an eye on hundreds of controls continuously and document them, which can be unbearable without automation.

It, therefore, becomes of dire importance that automated solutions that are able to deliver sustained and dependable tests of compliance in cloud environments are made possible. Automated compliance tools also facilitate the audit since they are used to identify anomalies in real time and the reports are automated in real time as well [14]. The tools also provide unified dashboards, which make it easy to monitor compliance in numerous cloud platforms. Also, they will allow them to adapt to changing regulatory frameworks without spending much money on manual updating. The policies are enforced with consistency across the services and regions as cloud infrastructure becomes dynamic and distributed, and automation ensures consistency even across regions.

D. Challenges in Multi-Cloud Migration

Multi-cloud migration implies flexibility, scalability, and such independence of vendors, yet poses a series of critical issues, which organizations should be capable of overcoming so that their transition would be secure and efficient [15]. These obstacles cut across technical, regulatory and operational lines, and it is, therefore, vital to undertake a strategic planning to succeed. The major issues are:

- **Complex Integration Across Platforms:** Multi-cloud migration requires integration of disparate cloud providers with different infrastructures, APIs and tools. The incompatibility of the networking, security, and data formats makes smooth interoperability a challenge that requires a thoughtful approach.
- **Security and Compliance Challenges:** policing uniform security controls and compliance across many realms of cloud is tough. Businesses need to enforce high-level encryption, access controls, and threat monitoring in an effort to safeguard sensitive data and conform to diverse regulatory policies [16].
- **Vendor Lock-In Risks:** Though the multi-cloud strategy is intended to prevent the concentration of all systems on a single access point, workload mobility is expensive and complicated. The organizations should also reduce lock-in by employing the open standards and APIs that guarantee interoperability and portability.
- **Performance and Latency Concerns:** The problem of performance and latency which arises due to workload placement in clouds. Companies have to optimize their distributions with frameworks such as edge computing, CDNs or hybrid infrastructures to distribute performance regionally.
- **Regulatory Complexity Across Regions:** Various industries and regions have various compliance requirements. To complicate multi-cloud migration, these diverse frameworks demand adjustments of strategies to meet the legal and regulatory anticipation of different organizations.

Overview Of Aws, Microsoft Azure And Gcp

The top three cloud service providers have broad ranges of infrastructure, platform solutions, and software solutions. AWS is characterized by wide global network with large service range and market leadership. Microsoft Azure is distinguished by its enterprise-focused solutions, robust hybrid cloud features, and smooth connectivity with other Microsoft products. GCP is a leader in big data analytics, machine learning, and developer-friendly tools, supported by Google's data and AI capabilities. Together, these platforms empower businesses with scalable, secure, and innovative cloud computing solutions.

A. AWS Macie

Currently leading the cloud computing platform industry is AWS, a subsidiary of Amazon.com, Inc. AWS is the most well-known cloud platform, offering a wide range of services to practically everyone, including governments, large corporations, and independent developers [17][18]. AWS started off as an internal cloud service. By 2006, it had evolved into a cloud platform that was openly available to the public, including services like Amazon S3 cloud storage and Elastic Compute Cloud (EC2). With over 200 fully functional services, AWS is now able to serve millions of clients and satisfy all their needs.

B. Microsoft Azure Purview

Microsoft Azure, formerly known as Windows Azure (Ffigure 2), is the company's public cloud computing platform. It renders colossal range of cloud services, including collaboration, storage, analytics, and computing. Users have a range of options for developing and expanding new apps or managing existing apps in the public cloud. Companies may utilize Azure platform to help them accomplish their goals and get past challenges. It serves a large number of Fortune 500 companies, e-commerce, and banking, and it offers open source technology-compatible solutions. With this flexibility, users may make use of the tools and technologies that they choose. Azure offers four services for cloud computing: IaaS, PaaS, SaaS, and serverless. Pay-as-you-go (PAYG) pricing is how Microsoft bills for Azure, so customers only pay for the resources and services they utilize each month.

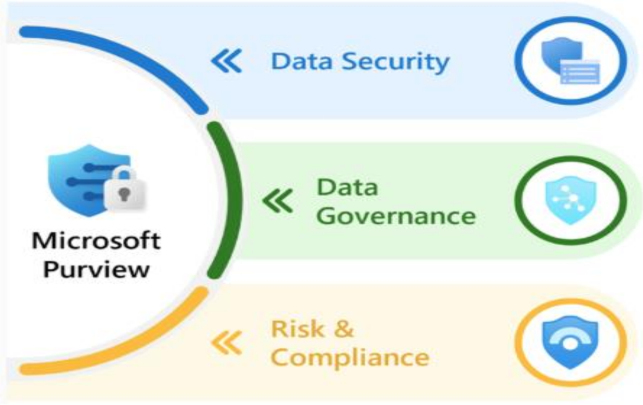

Figure 2. Microsoft Azure

C. Google Cloud

In general, GCP refers to the group of cloud computing services that are provided to people and businesses who want to build their own digital cloud infrastructures. GCP is used by notable sites including YouTube, Gmail, and the generative AI Google Chatbot Bard. ML (machine learning), compute, data analytics, and data storage are among the cloud computing services offered by GCP [19][20]. Google offers a public cloud computing service known as GCP. Its numerous services encompass computing, networking, storage, big data, developer tools, IoT, cloud AI, data transmission, identification and security, and cloud computing. GCP is a worldwide acknowledged corporation. Google Cloud Platform is characterized by high security, while it also provides enhanced networking capabilities and a more favorable price structure, as seen in Figure 3.

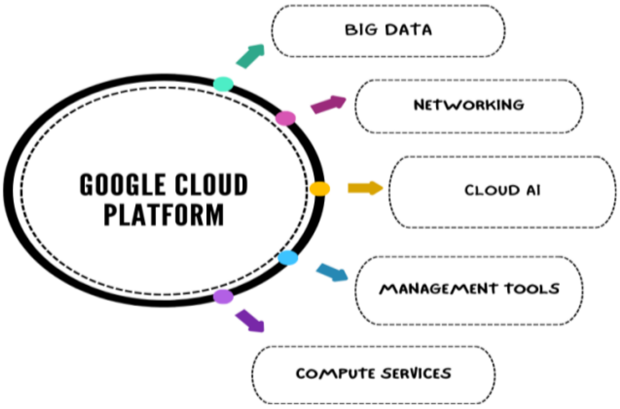

Figure 3. Google Cloud Platform

D. Benefits of AWS, Azure, And GCP

There are some benefits of different cloud computing tools are:

- AWS offers a robust, scalable, and secure cloud infrastructure that supports dynamic workloads through features like Auto Scaling and Elastic Load Balancing. It provides significant cost savings with Reserved Instances up to 72% compared to On-Demand pricing and flexibility through Convertible Reserved Instances [21][22]. AWS supports learners and professionals via AWS Educate, offering free credits, labs, and a student portal. Organizations in the AWS Specialization Partner Program gain access to expert guidance, exclusive roadmaps, and financial incentives, making AWS a comprehensive solution for enterprises of all sizes.

- Microsoft Azure is known for its strong hybrid cloud capabilities and cost-efficiency. Through Azure Migration and Modernization Program (AMMP), organizations receive free credits, technical consulting, and migration support [23]. Azure Hybrid Benefits allow cost optimization by reusing existing Windows, Linux, or SQL Server licenses. Extended security updates are available for older workloads like Windows Server 2008 when migrated to Azure. Azure also provides discounted services for development and testing environments through Visual Studio subscriptions, along with $100–$150 in credits for students and grants for educational institutions and NGOs.
- Google Cloud Platform (GCP) excels in data analytics, big data processing, and AI/ML workloads. Its Partner Advantage Program provides organizations of all levels access to training, access to incentives, and Google Workspace discounts, the highly comprehensive benefits of which are available to Premier Partners. GCP supports cloud education through Google Cloud Skills Boost, providing 200 free credits annually for students to access online labs, courses, and structured learning paths. These features make GCP particularly attractive to data-driven organizations and academic communities looking for cloud-based innovation and skill development.

Comparative Study Of Gcp, Aws And Microsoft Azure

The top cloud providers are AWS, Azure, and GCP; each offers colossal range of services with different advantages. Founded in 2006, AWS has the biggest market share (32%) and is renowned for its extensive service offering, comprehensive feature set, and high availability.[24]. Azure, which was first released in 2010, is perfect for current Microsoft consumers since it effortlessly interacts with Microsoft products. Launched in 2008, GCP excels in analytics and open-source integration and provides user-friendly interfaces.

All platforms support secure, scalable, and highly available infrastructure with similar pricing models. While AWS and Azure have a steeper learning curve, GCP is more intuitive. Their core services such as data warehousing, computing, and storage are robust, with Redshift, Synapse, and Big Query leading in data analytics solutions. All three support pay-as-you-go pricing and compliance-driven security (see Table I)

TABLE I. COMPARISON OF DIFFERENT CLOUD COMPUTING TOOLS[21]

Parameters	AWS	AZURE	GCP
Launch Year	2006	2010	2008
Market Share	32	23	10
Pricing	Pay-as-you-Go Reserved Instances Spot Pricing	Pay-as-you-Go Reserved Instances Spot Pricing	Pay-as-you-Go Committed use discounts Sustained use discounts
Performance	Highly Performance Highly Performance High Availability	Highly Performance Scalable High Availability	Highly Performance Scalable High Availability

Parameters	**AWS**	**AZURE**	**GCP**
Features	Rich feature set Wide range of services Large Ecosystem	Rich feature set Wide range of services Large Ecosystem	Rich feature set Wide range of services Large Ecosystem
User Interface	Robust Steep Learning Curve	Robust Steep Learning Curve	User-friendly Easy to use
Security	Highly secure Compliance with regulations	Highly secure Compliance with regulations	Highly secure Compliance with regulations
Support	Extensive	Extensive	Extensive
Integration	Extensive third-party support	Seamless with Microsoft Products	Best with Google Services, good for open-source tools
Usability	Feature-rich, steeper learning	User-friendly, Ideal for Microsoft Users	Intuitive, user-friendly console
Data Warehousing	Amazon Redshift	Azure Synapse Analytics	Big Query
Computer	Amazon EC2 Instances	Azure virtual machines	Compute Engine
Storage	AWS Simple Storage Service	Azure Blob Storage	Cloud Storage
Networking	Virtual Private Cloud	Virtual Network	Virtual Private Cloud

A. Comparison Analysis Framework of AWS, Microsoft Azure And GCP

AWS, Microsoft Azure, and CGP—three of most well-known cloud computing platforms—will be contrasted.

- **Pricing:** Among the many price options offered by the three platforms are pay-per-use, reserved instances, and spot instances. GCP has the lowest price, whereas AWS has the highest.[25]. Nevertheless, the price might change based on good or service being used.
- **Performance:** The three systems render superior scalability, reliability as well as availability. AWS, in its turn, has been leading this market long because of abundance of data centers as well as rich portfolio of services.
- **Features:** AWS offers greatest number of features, although every platform offers particular features and services. Microsoft Azure is pioneering in the field of hybrid cloud and AI/ML whereas GCP is famous in terms of big data and analytics [26].
- **User Interface:** Easy-to-decipher user interfaces exist on all platforms and the most complex one is that which is present on Amazon which is difficult to navigate by a casual user. The interface of Microsoft Azure is less complicated, whereas GCP is more modern and less structured [27].
- **Security:** The three platforms are very secure; however, AWS offers the most detailed security and certification. Microsoft Azure can also provide a powerful security system despite the

fact that GCP is famed for using encryption and safe networking.

- **Support:** All platforms offer a different degree of support, with the possibility to go from community forums to paid continuous service. AWS offers the most supportive community, whereas Google Cloud Platform and Microsoft Azure offer the same support.
- **Integration Capabilities:** Strong integration with Google's services and open-source tools allows GCP to support machine learning and data analytics applications. It may take more effort to integrate with non-Google services.
- **Usability:** GCP's console is commended for being user-friendly and intuitive, making it appropriate for users who are not familiar with cloud services.
- **Compute Services:** Application code may be hosted by businesses using AWS, Azure, and GCP, among other possibilities. In this context, "Compute" refers to the application's resource hosting model.
- **Storage Services:** AWS, Azure, and GCP render a colossal range of services, encompassing data storage for virtual machine (VM) discs.
- **Networking:** You can use a range of networking options from AWS, Azure, and GCP either separately or in combination.
- **Data Warehouse:** A data warehouse stores raw data, metadata, summary data, and processed operational data in one location for easy user access. Data warehouse options are available from AWS, Azure, and GCP.

Literature Review

This literature Summary examines recent advancements in automated compliance within multi-cloud environments. Table II of the research highlights the following: Author, Study On, Approach, Key Findings, Challenges, and Future Directions.

Patil (2025) the possibility of blockchain delineating immutable audit trails, secure transaction records, and automated compliance verification. Our approach integrates blockchain protocols into the AWS and Azure environments to increase trust and transparency while reducing the inherent vulnerabilities of distributed cloud systems. It can show, through a series of experiments and analyses, that blockchain not only streamlines the enforcement of security policies but also improves incident response times to amortize risk of data breaches and unauthorized access [28].

Man and Tai (2024) data encryption and privacy protection technologies in cloud computing environments. By systematically implementing and evaluating various encryption algorithms (such as AES, RSA, and homomorphic encryption) and privacy protection techniques (including data masking, differential privacy, secure multi-party computation, and zero-knowledge proofs), the feasibility and effectiveness of these technologies in cloud environments are explored. A simulated cloud environment was constructed for experiments, and the results indicate that AES performs excellently in large-scale data processing, while homomorphic encryption demonstrates unique advantages in specific scenarios [29].

Yu (2024) the differences in data integrity, privacy and operating efficiency of various cryptographic algorithms, as well as their adaptability in a cloud computing environment. The experimental results stipulate that compared with traditional methods, the encryption and decryption speed of the algorithm can be increased by about 15%, and the execution efficiency of smart contracts can be increased by about 12%. To ameliorate the security and privacy of data sharing, this project intends to study a data sharing security algorithm based on blockchain in a cross-cloud computing environment. The security algorithm that integrates cryptography and smart contracts is studied to ensure that data is effectively encrypted during the sharing process, and to corroborate execution efficacy and effectiveness of smart contracts under dynamic changes of the sharing parties [30].

Morello et al. (2024) a privacy-preserving regulatory compliance verification mechanism has been included and put into practice in a use case to confirm that GDPR article 32 is being followed. It offers a regulatory verification protocol that is based on the attribute verification protocol and only discloses the entity's compliance, not any personal information. Our findings show that the suggested approach may effectively have an external validator confirm an entity's regulatory compliance. In order to verify regulatory compliance, the verifier might have to get confidential data that could jeopardize the privacy of the businesses being checked. Thus, in order to verify that companies are in compliance with legislation like the GDPR, the regulatory compliance verification process must protect those businesses' privacy. [31].

Suwardi Ansyah et al. (2023) The contemporary technology industry is dominated by the Internet of Things (IoT), a new communication technology that has developed quickly. IoT's ease of access to colossal range of devices has sparked the creation of new apps that produce many data points from numerous things. The implementation of IoT requisites a protocol that is compact, has fast response times, and has good communication performance. MQTT is a machine-to-machine communication protocol that is ideal for the Internet of Things, as it can transmit data quickly and efficiently with minimal bandwidth requirements. Three primary parts make up MQTT the Publisher, the Broker, and the Subscriber. IoT devices, called publishers, deliver sensor data on a regular basis to subscribers, who are typically data subscription apps [32].

Liu, Xin and Dai (2022) Due to the quick advancement of cloud apps and virtualization technologies, cloud disaster recovery services are becoming the most popular choice for data disaster recovery research and implementation. The demands of customers for data security backup cannot be satisfied by single-cloud disaster recovery services because of technical problems, administrative errors, network attacks, natural calamities, etc. Multi-cloud and heterogeneous cloud environments are required for the deployment of disaster recovery systems in order to execute cross-cloud disaster restoration and multi-cloud retention of data[33].

Joshi et al. (2022) the benefits, difficulties, and potential avenues for further study on safe data processing and exchange in loud environment. The underlying reason of widespread issue is increasing use of cloud computing by several enterprises. Therefore, utilizing any device to load and receive data from cloud providers' facilities raises a variety of security and privacy concerns, such as data loss, theft, and manipulation. Insiders obtaining unauthorized access is one of the main problems that might occur. Although there are a number of strategies to stop cloud administrators from obtaining unauthorized access, these strategies haven't proven effective in intercepting them from accessing customer data stored in the cloud[34]

TABLE II. SUMMARY OF A STUDY ON AUTOMATED COMPLIANCE ENFORCEMENT IN MULTI-CLOUD DATABASE ENVIRONMENTS

Author”	Study On”	Approach”	Key Findings”	Challenges”	Future Directions”
Patil (2025)	Blockchain for audit and	Integrated blockchain with	Improved transparency, faster incident response,	Complexity in integrating	Optimize blockchain

Author”	**Study On”**	**Approach”**	**Key Findings”**	**Challenges”**	**Future Directions”**
	compliance in multi-cloud	AWS and Azure for immutable audit trails and policy enforcement	reduced data breach risks	blockchain into distributed cloud systems	integration for scalability and real-time compliance
Man and Tai (2024)	Encryption and privacy protection in cloud computing	Tested AES, RSA, homomorphic encryption, and privacy techniques in a simulated cloud environment	AES excels in large-scale processing; homomorphic encryption effective in selective use cases	Performance overhead in privacy-preserving methods	Improve computational efficiency of homomorphic encryption and multi-party computation
Yu (2024)	Cryptography and smart contracts in cross-cloud environments	Developed a secure data sharing algorithm integrating cryptography with blockchain-based smart contracts	15% faster encryption/decryption; 12% better smart contract execution efficiency	Ensuring secure and efficient contract execution under dynamic party changes	Enhance adaptability and scalability of the cryptographic smart contract model
Morello et al. (2024)	GDPR-compliant regulatory verification protocol	Designed a privacy-preserving attribute-based verification protocol for GDPR Article 32	External verifiers can confirm compliance without accessing private data	Verifiers may need sensitive data that poses privacy risks	Broaden protocol for wider regulatory contexts while maintaining privacy
Suwardi Ansyah et al. (2023)	IoT communication protocols (MQTT)	Analysis of MQTT protocol and its components (Publisher, Broker, Subscriber) for efficient IoT	MQTT is lightweight, low-bandwidth, and ideal for real-time machine-to-machine communication	Limitations in handling large-scale or complex IoT deployments	Enhance MQTT to support scalable, secure multi-device IoT environments

Author"	Study On"	Approach"	Key Findings"	Challenges"	Future Directions"
		communication			
Liu, Xin and Dai (2022)	Cloud disaster recovery using multi-cloud settings	Proposed multi-cloud and heterogeneous disaster recovery strategies	Improved fault tolerance and security over single-cloud systems	Integration complexity and vulnerability to network attacks or natural disasters	Develop AI-driven cross-cloud disaster recovery frameworks
Joshi et al. (2022)	Safe data processing and insider threats in cloud	Reviewed risks in cloud data sharing and existing privacy measures	Insider access and unauthorized data manipulation remain persistent challenges	Ineffectiveness of current prevention methods against insider threats	Innovate trustworthy execution environments and zero-trust architectures

Conclusion And Future Work

The digital environment has been transformed by cloud computing through the provision of versatile, economical, and flexible IT networks. Since more and more organizations have adopted and are currently using multi-cloud environments, data compliance has become a key issue of concern with different rules and regulations in different countries as well as technicality arising from how best to integrate the platforms. The paper has given a general understanding of data compliance in multi-cloud architectures which considers regulatory requirements, GDPR, and HIPAA. It has observed the obstacles and the possible solutions surrounding the automation of compliance automation and cloud migration administration. The comparative scrutiny of AWS, Microsoft Azure and GCP brings out their strong points, features, and where they fit in various organizational requirements. AWS is ahead of the pack by having a vast ecosystem and well-developed infrastructure, whereas Azure is the preferred choice of the enterprise, and recognizable for its hybrid models, and GCP stands out by having strong analytics and machine learning features. The comparison framework provides beneficial insights to the stakeholders to make informed decisions based on the cost, performance, usability, security, and integrations capabilities.

Future research in this area could be oriented towards the evolution of consolidated compliance management systems capable of operation with multi-heterogeneous cloud platforms. Moreover, progressive compliance analytics enabled by AI and ML can become a game-changer in detecting a possible regulatory violation in real-time. One of them is the implementation of blockchain technologies that can be used to create immutable audit trails of cloud transactions and can ultimately increase transparency, traceability, and trust of multi-cloud deployments. Streamlining compliance procedures as well as encouraging cooperation among cloud providers and regulatory authorities will also play an important role in streamlining compliance procedures in future cloud environments.

References

[1]. V. Goyal and A. Kumar, “Review Paper On Comparison Of AWS, Microsoft Azure And Google Cloud Platform,” Int. Res. J. Mod. Eng. Technol. Sci., vol. 5, no. 12, 2023.

[2]. K. Evans, E. Stewart, and G. Foster, “Comprehensive Review of Cloud-Driven Machine Learning: A Comparative Analysis of AWS, Azure, and Google Cloud,” 2025.

[3]. V. Shah, “Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 877–885, 2023, doi: https://doi.org/10.32628/IJSRCSEIT.

[4]. P. Somasundaram, “Navigating Regulatory Compliance in Multi-Cloud Environments: Challenges and Technological Solutions,” Int. J. Core Eng. Manag., vol. 7, no. 2, 2022.

[5]. A. Bhad, “Security and Compliance Challenges in Multi-Cloud Environments: A Comparative Study of Industry-Specific Strategies,” no. August, 2025.

[6]. H. A. Imran et al., “Multi-Cloud: A Comprehensive Review,” in 2020 IEEE 23rd International Multitopic Conference (INMIC), IEEE, Nov. 2020, pp. 1–5. doi: 10.1109/INMIC50486.2020.9318176.

[7]. P. Borra and H. P. Pamidipoola, “Serverless Computing: The Future of Scalability and Efficiency with AWS, Azure, and GCP,” Int. J. Adv. Res. Sci. Commun. Technol., no. April, pp. 505–514, Feb. 2025, doi: 10.48175/IJARSCT-23373.

[8]. P. Borra, “Comparative Review: Top Cloud Service Providers ETL Tools -AWS vs. Azure vs. GCP,” SSRN Electron. J., no. June, 2024, doi: 10.2139/ssrn.4914175.

[9]. A. Folorunso, O. Babalola, C. E. Nwatu, and A. Adedoyin, “A comprehensive model for ensuring data compliance in cloud computing environment,” World J. Adv. Res. Rev., vol. 24, no. 2, pp. 1983–1995, Nov. 2024, doi: 10.30574/wjarr 2024.24.2.3514.

[10]. L. Campbell, “Security Compliance in Cloud Computing (e.g., GDPR, HIPAA),” 2025.

[11]. D. Patel, “The Role of Amazon Web Services in Modern Cloud Architecture: Key Strategies for Scalable Deployment and Integration,” Asian J. Comput. Sci. Eng., vol. 9, no. 4, pp. 1–9, 2024.

[12]. S. Tewari and A. Chitnis, “AI and Multi-Cloud Compliance : Safeguarding Data Sovereignty,” vol. 7, no. 7, pp. 571–587, 2024.

[13]. D. Antiya and O. Corporation, “Compliance as Code: Automating Compliance in Cloud Systems,” Int. J. Recent Innov. Trends Comput. Commun., vol. 8, no. February, 2025.

[14]. V. Shah, “Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks,” ESP J. Eng. Technol. Adv., vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[15]. A. Chennupati, “Challenges and Best Practices in Multi Cloud Migration for Enterprises,” vol. 7, no. 4, pp. 504–510, 2023.

[16]. N. Patel, “Secure Access Service Edge (SASE): Evaluating The Impact Of Converged Network Security Architectures In Cloud Computing,” J. Emerg. Technol. Innov. Res., vol. 11, no. 3, 2024.

[17]. M. P. Patel and M. S. Gajjar, “Cloud Wars: A Comparative Study of AWS, Azure And Google Cloud,” Int. Res. J. Mod. Eng. Technol. Sci., vol. 5, no. 10, 2023.

[18]. D. Patel, “Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.

[19]. A. Mishra, “AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT

Network," Int. J. Adv. Eng. Manag., vol. 7, no. 3, pp. 05–13, 2025.

[20]. S. S. S. Neeli, "Securing and Managing Cloud Databases for Business - Critical Applications," J. Eng. Appl. Sci. Technol., vol. 7, no. 1, p. 6, 2025.

[21]. P. Borra, "Comparison and Analysis of Leading Cloud Service Providers (AWS, Azure and GCP)," Int. J. Adv. Res. Eng. Technol., vol. 15, no. 3, pp. 266–278, 2024, doi: 10.2139/ssrn.4914145.

[22]. M. Menghnani, "Modern Full Stack Development Practices for Scalable and Maintainable Cloud-Native Applications," vol. 10, no. 2, 2025, doi: doi.org/10.5281/zenodo.14959407.

[23]. S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Network.," J. Crit. Rev., vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[24]. G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," Int. J. Curr. Eng. Technol., vol. 15, no. 3, 2025.

[25]. A. Chauhan, "A Comparative Study of Cloud Computing Platforms," Turkish J. Comput. Math. Educ., vol. 11, no. 1, pp. 821–826, 2020, doi: 10.17762/turcomat.v11i1.13563.

[26]. O. A. Alqahtani and M. Alsandouny, "Comprehensive Comparison of Cloud Storage: GCP, AWS, AND AZURE," Int. J. Eng. Res. Appl. www.ijera.com, vol. 15, no. 3, pp. 27–35, 2025, doi: 10.9790/9622-15032735.

[27]. S. Garg, "Predictive Analytics and Auto Remediation using Artificial Intelligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019.

[28]. B. Patil, "Integration of Blockchain with AWS and Azure for Enhanced Cloud Security and Compliance in Multi-Cloud Architectures," in 2025 International Conference on Computing and Communication Technologies (ICCCT), 2025, pp. 1–5. doi: 10.1109/ICCCT63501.2025.11018983.

[29]. D. Man and H. Tai, "Research on Data Encryption and Privacy Protection Technologies in Cloud Computing Environments," in 2024 International Conference on Information Technology, Communication Ecosystem and Management (ITCEM), 2024, pp. 145–150. doi: 10.1109/ITCEM65710.2024.00035.

[30]. X. Yu, "Research on Security Algorithm of Cross-Cloud Data Sharing Supported by Blockchain," in 2024 IEEE 2nd International Conference on Electrical, Automation and Computer Engineering (ICEACE), 2024, pp. 1308–1312. doi: 10.1109/ICEACE63551.2024.10899028.

[31]. M. Morello, P. Sainio, and M. Alshawki, "Regulatory Compliance Verification: A Privacy Preserving Approach," in 2024 8th Cyber Security in Networking Conference (CSNet), 2024, pp. 263–267. doi: 10.1109/CSNet64211.2024.10851761.

[32]. A. S. S. Ansyah et al., "MQTT Broker Performance Comparison between AWS, Microsoft Azure and Google Cloud Platform," in 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), IEEE, Feb. 2023, pp. 1–6. doi: 10.1109/ICRTEC56977.2023.10111870.

[33]. B. Liu, Y. Xin, and S. Dai, "Blockchain-based Disaster Recovery Data Storage and Security Auditing Solution in Multi-cloud Environment," in 2022 International Applied Computational Electromagnetics Society Symposium, ACES-China 2022, 2022. doi: 10.1109/ACES-China56081.2022.10065296.

[34]. A. Joshi, A. Raturi, S. Kumar, A. Dumka, and D. P. Singh, "Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks," in 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), 2022, pp. 230–233. doi: 10.1109/ICFIRTP56122.2022.10063186.