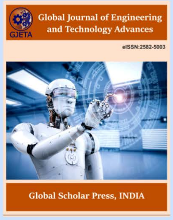
Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/


Global Journal of Engineering and Technology Advances
GJETA
eISSN:2582-5003
Global Scholar Press, INDIA

(Research Article)

Policy framework for Cloud Computing: AI, governance, compliance and management

Olufunbi Babalola [1], Adebisi Adedoyin [2], Foyeke Ogundipe [3], Adebola Folorunso [4] and Chineme Edger Nwatu [5, *]

[1] *Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA 15213, USA.*
[2] *Bournemouth University Department of Information Technology United Kingdom.*
[3] *SPS Division of Programs in Business, Department of Management and Technology, New York University.*
[4] *School of Business, Technology and Health Care Administration Capella University, Minneapolis, MN, USA 55402, USA.*
[5] *Western Illinois University School of Computer Sciences Stripes Hall 44, 1 University Circle Macomb IL 61455-1390 USA.*

Global Journal of Engineering and Technology Advances, 2024, 21(02), 114–126

Publication history: Received on 07 October 2024; revised on 19 November 2024; accepted on 21 November 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.2.0212

Abstract

The rapid evolution of cloud computing has transformed data management, operational efficiency, and artificial intelligence (AI) capabilities across industries. However, this advancement presents new challenges in governance, compliance, and management, necessitating a comprehensive policy framework to ensure secure, ethical, and effective cloud usage. This review examines a robust policy framework designed to address these challenges, focusing on the integration of AI, governance practices, regulatory compliance, and cloud management. The framework outlines specific policies for AI, emphasizing ethical considerations, accountability, and transparency, alongside mechanisms for privacy and bias mitigation to foster responsible AI deployment in cloud environments. Governance policies are structured to establish clear data stewardship, risk management, and continuous monitoring protocols, ensuring that cloud resources align with organizational and regulatory standards. Moreover, compliance is addressed through adherence to global standards such as GDPR and HIPAA, with an emphasis on data sovereignty, auditability, and vendor accountability to maintain regulatory alignment across jurisdictions. Management policies within the framework focus on optimizing resource allocation, enforcing Service Level Agreements (SLAs), and developing disaster recovery and business continuity strategies. These management policies aim to balance cost-efficiency with performance reliability. Recognizing the complexities of multi-cloud and hybrid environments, the framework proposes adaptable guidelines that accommodate rapid technological shifts and address security and privacy risks inherent in cloud computing. Through case studies and best practices, this framework offers actionable insights for organizations seeking to implement secure, compliant, and efficient cloud systems. In exploring the future landscape, the review anticipates emerging regulations and underscores the importance of industry-wide collaboration in refining cloud policies. This policy framework provides a foundation for organizations to harness the full potential of cloud computing while upholding standards in AI ethics, data governance, and regulatory compliance.

Keywords: Policy Framework; Cloud Computing; Artificial intelligence; Governance

1. Introduction

Cloud computing has fundamentally changed the landscape of information technology, reshaping how businesses, governments, and individuals store, manage, and access data (Benlian *et al.*, 2018). As a service model, cloud computing offers on-demand computing resources and services over the internet, eliminating the need for physical infrastructure and enabling rapid scaling to meet fluctuating demands. The cloud computing model can be categorized into three main service types: Infrastructure as a Service (IaaS), which provides fundamental computing resources; Platform as a Service (PaaS), which enables users to deploy applications without managing the underlying infrastructure; and Software as a Service (SaaS), which provides access to complete software solutions on a subscription basis. The

[*] Corresponding author: Chineme Edgar Nwatu

applications of cloud computing are diverse, spanning sectors such as finance, healthcare, education, and e-commerce (Bello *et al.*, 2021). Its benefits include cost-efficiency, scalability, and accessibility, which have led to widespread adoption across the globe. In recent years, cloud services have grown rapidly, and the global market is projected to continue expanding as more organizations rely on cloud-based platforms to drive digital transformation (Kommisetty, 2022).

Despite its advantages, the accelerated growth of cloud computing introduces several challenges, particularly in areas such as data security, regulatory compliance, and the ethical deployment of advanced technologies like artificial intelligence (AI) (Kumar, 2022). These challenges highlight the need for a comprehensive policy framework to govern cloud computing practices effectively. As organizations increasingly integrate AI into cloud environments to enhance data processing and decision-making capabilities, concerns about data privacy, ethical AI use, and regulatory adherence become more pronounced. Without a structured approach, the potential risks such as data breaches, algorithmic bias, and non-compliance with international standards could overshadow the benefits of cloud computing (Benson *et al.*, 2021). Therefore, a well-defined policy framework is essential to guide organizations in implementing secure, compliant, and ethically sound cloud strategies (Mahajan, 2023).

This review aims to address the need for a policy framework for cloud computing, focusing on four key areas: AI integration, data governance, regulatory compliance, and effective cloud management. Each of these areas is critical for ensuring that cloud resources are utilized safely, efficiently, and responsibly. AI integration policies will explore the ethical considerations and accountability measures necessary to deploy AI systems that are transparent and unbiased. Data governance policies will establish guidelines for managing data ownership, access rights, and stewardship within the cloud, ensuring that data integrity and privacy are preserved. Regulatory compliance will focus on adherence to regional and international standards, such as GDPR and HIPAA, addressing issues such as data sovereignty and cross-border data flows. Finally, management policies will focus on optimizing cloud resources through effective resource allocation, Service Level Agreements (SLAs), and disaster recovery planning, aiming to create a sustainable and resilient cloud environment. The policy framework presented in this review is designed to provide organizations with a structured approach to navigating the complexities of cloud computing. By establishing guidelines for AI, governance, compliance, and management, this framework aims to mitigate risks and enable organizations to maximize the benefits of cloud technology while upholding ethical and regulatory standards. With the rapid advancement of cloud computing technologies, a cohesive and adaptable policy framework is essential to support secure and sustainable cloud adoption (Angel *et al.*, 2021). This introduction sets the stage for a detailed exploration of each policy area, offering insights and best practices to guide organizations in building robust cloud infrastructures that align with industry standards and regulatory expectations.

2. Policy Framework for AI in Cloud Computing

The integration of artificial intelligence (AI) into cloud computing has unlocked new possibilities for data processing, automation, and decision-making (Kanungo, 2020). However, this integration raises critical concerns about ethics, accountability, privacy, bias, and effective management of AI systems. A comprehensive policy framework is essential to guide organizations in navigating these challenges, ensuring AI's responsible, secure, and equitable deployment within cloud environments.

The rapid deployment of AI technologies in the cloud requires an ethical framework that prioritizes transparency and accountability as illustrated in figure 1 (Dondapati *et al.*, 2022). Ethical AI use within cloud computing involves designing systems that respect human rights, privacy, and autonomy while preventing misuse or harmful outcomes (Ahmad *et al.*, 2022). Key aspects of an ethical framework include establishing clear accountability for AI decisions, ensuring AI's alignment with societal norms, and implementing mechanisms for transparency in AI processes. This framework should outline the responsibilities of AI developers, cloud providers, and end-users, ensuring that ethical standards are upheld across all stages of AI implementation. Additionally, organizations must establish a transparent process for explaining AI-driven decisions, which builds trust among stakeholders and addresses potential ethical dilemmas.

Data privacy and security are crucial considerations for AI applications in cloud environments, as AI algorithms typically rely on vast amounts of sensitive data to learn and make decisions (Kavitha *et al.*, 2021). To mitigate privacy risks, a strong policy framework should enforce data protection measures that align with regulatory standards like GDPR and HIPAA. Key components include data anonymization, encryption, and access controls to protect sensitive information. Policies should also address the specific risks associated with AI, such as the potential for unintended data inference and model inversion attacks, which can reveal private information about individuals within a dataset. By implementing robust security practices, organizations can protect against data breaches, unauthorized access, and ensure that sensitive data remains secure throughout the AI lifecycle.

Bias in AI algorithms is a significant concern, particularly when these models are deployed on a large scale through cloud platforms (Hardt *et al*., 2021). AI bias can result from skewed data, faulty algorithms, or underlying systemic issues, leading to unfair or discriminatory outcomes. To address this, the policy framework should include guidelines to identify and mitigate bias at every stage of AI model development and deployment. Techniques like dataset balancing, fairness-aware machine learning, and regular audits of AI outcomes can help minimize bias. Additionally, organizations should establish transparency in data collection and feature selection, ensuring that models are trained on diverse, representative datasets. Policies promoting fairness in AI reinforce equitable treatment and reduce the risk of discriminatory practices in cloud-deployed AI applications (Perifanis and Kitsios, 2022).

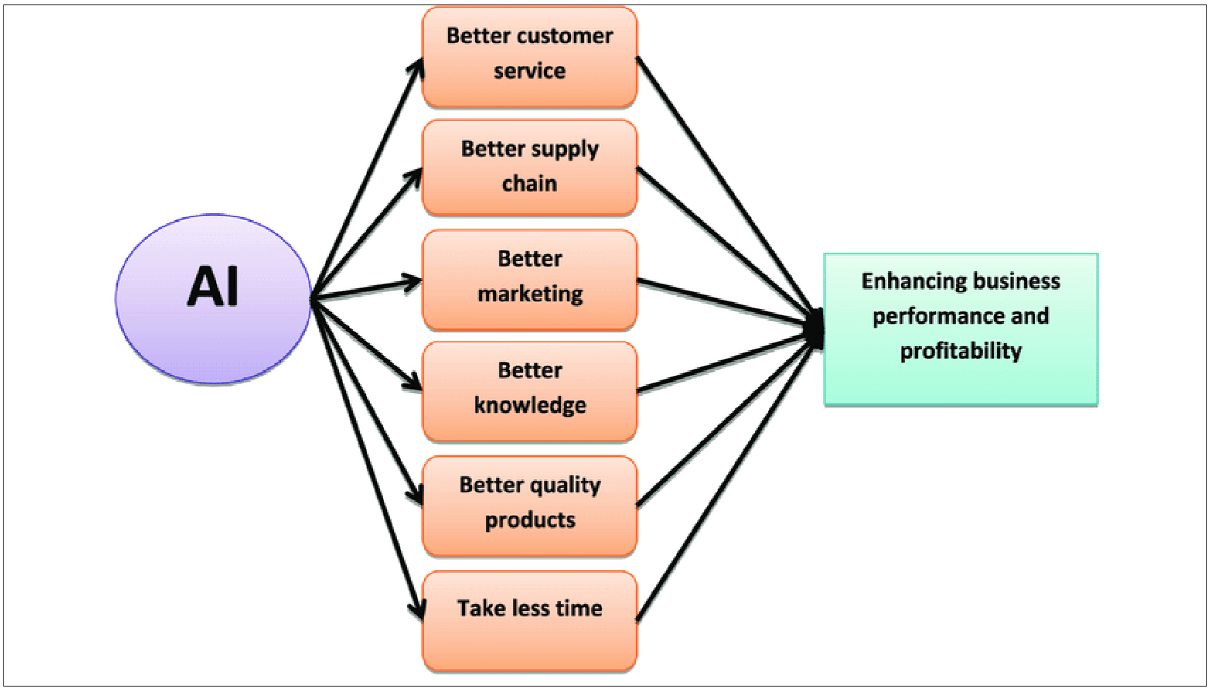


Figure 1 Framework for artificial intelligence (Dondapati *et al*., 2022)

Effective AI lifecycle management policies are essential to ensure the quality, reliability, and accountability of AI models within cloud environments. AI lifecycle management encompasses model development, deployment, monitoring, and retirement. Policies should require rigorous testing of AI models before deployment, including checks for accuracy, fairness, and potential risks (Kaur *et al*., 2022). Once deployed, AI systems must be continuously monitored to detect issues or performance degradation over time. Monitoring mechanisms should include automated alerts for significant deviations in model behavior, particularly for critical applications like healthcare or finance. Additionally, policies should specify criteria for model updates and the retirement of obsolete models, preventing outdated or ineffective algorithms from affecting decision-making. Lifecycle management also includes version control, documentation, and clear accountability protocols, ensuring traceability across the model's lifecycle (Wohlrab *et al*., 2002). This enables organizations to make informed adjustments, thereby increasing AI's reliability and adaptability within the cloud.

A well-defined policy framework for AI in cloud computing is crucial for harnessing AI's full potential while addressing ethical, privacy, fairness, and management challenges (Machireddy *et al*., 2021). By setting standards for AI ethics, data privacy, bias mitigation, and lifecycle management, organizations can ensure that AI applications in the cloud are transparent, secure, and fair. This framework not only protects users and organizations but also fosters trust in AI systems, supporting responsible innovation in cloud computing. As AI and cloud technologies evolve, continuous policy refinement will be essential to address emerging risks and maintain robust, accountable, and ethical AI systems in the cloud.

2.1. Governance in Cloud Computing

Effective governance in cloud computing is essential to manage the complexity of cloud environments, ensure data security, and uphold regulatory compliance (Shah and Konda, 2022). A comprehensive governance framework provides guidelines that help organizations structure and manage cloud resources, define roles and responsibilities, and establish oversight mechanisms. With increasing reliance on cloud platforms, strong governance practices are necessary to control data access, mitigate risks, and maintain a secure, transparent, and well-regulated cloud environment.

Cloud governance principles serve as foundational guidelines to define roles, responsibilities, and accountability across cloud operations (Jaatun *et al.*, 2020). These principles establish a structured approach to decision-making, resource allocation, and compliance within cloud environments. Key governance principles include defining clear roles for stakeholders, such as cloud administrators, data custodians, and compliance officers, who are responsible for overseeing cloud usage and ensuring that it aligns with organizational goals and regulations. Additionally, oversight mechanisms like governance committees or cloud-specific compliance teams help in monitoring cloud policies and aligning them with business objectives. By clearly outlining the responsibilities and functions of each role, cloud governance principles promote accountability and streamline decision-making processes, enabling organizations to operate cloud environments effectively and in line with established standards.

In a cloud-based framework, data stewardship and ownership policies are critical for defining control and responsibility over data. Data stewardship refers to the management, oversight, and protection of data assets, while ownership implies control and access rights to the data (Manohar *et al.*, 2020). Cloud governance should include policies that clearly delineate the responsibilities of both cloud providers and customers in terms of data access, security, and compliance. This involves defining who owns the data stored in the cloud and who is responsible for data protection, privacy, and integrity. For instance, in a multi-tenant cloud environment, data ownership policies should specify which entities have access to shared resources and how data segmentation is maintained to prevent unauthorized access. Additionally, data stewardship practices should include guidelines for data classification, labeling, and management, ensuring that sensitive data is handled in accordance with regulatory requirements. This approach reinforces accountability in data handling and strengthens security protocols within cloud ecosystems.

Risk management is a crucial aspect of cloud governance, focusing on identifying, assessing, and mitigating risks associated with cloud operations. Cloud environments are prone to various risks, including operational disruptions, security vulnerabilities, and financial uncertainties (Stein *et al.*, 2020). A well-defined risk management framework should outline specific policies and controls to manage these risks. This framework includes strategies for assessing potential risks before cloud adoption, such as evaluating vendor reliability, security protocols, and regulatory compliance. Operational risks, for instance, can be mitigated by implementing robust disaster recovery and business continuity plans that ensure data availability and system resilience. Security risks, including data breaches and cyberattacks, can be minimized by enforcing access controls, encryption, and multi-factor authentication. Financial risks are managed by tracking resource utilization and aligning cloud expenses with budgetary limits. By proactively addressing these risks, organizations can protect their cloud assets and ensure stable, uninterrupted service delivery.

Continuous monitoring and auditing are integral components of cloud governance that ensure compliance with established policies and enable quick detection of deviations (Torkura *et al.*, 2021). Automated and manual auditing processes play a crucial role in maintaining cloud security, performance, and adherence to governance standards. Continuous monitoring involves using automated tools to track system activity, detect anomalies, and alert administrators to potential threats or policy violations. This real-time approach allows organizations to respond promptly to security incidents or operational disruptions. Periodic manual audits, on the other hand, provide deeper insights into system performance and policy adherence, allowing organizations to refine governance practices based on audit findings. For instance, a quarterly audit might examine data access logs, verify compliance with regulatory standards, and assess the effectiveness of security controls. By integrating both automated monitoring and manual auditing, organizations can maintain a high level of oversight and accountability within cloud environments, ensuring that governance standards are consistently met (Ali *et al.*, 2020; Dittakavi, 2022).

Effective governance in cloud computing provides a structured approach to managing cloud resources, protecting data, and mitigating risks. Through well-defined governance principles, organizations can clarify roles and responsibilities, establish data stewardship and ownership policies, and implement risk management strategies. Continuous monitoring and auditing processes further support these governance efforts by ensuring ongoing compliance and enabling rapid response to any issues (Cardoni *et al.*, 2020). A strong governance framework not only secures cloud environments but also aligns them with organizational goals and regulatory requirements, fostering a robust and resilient cloud infrastructure. As cloud computing continues to evolve, adaptable governance practices will remain essential for ensuring that cloud operations are safe, compliant, and efficient.

2.2. Compliance and Regulatory Policies in Cloud Computing

As cloud computing continues to expand globally, compliance and regulatory policies play a critical role in ensuring the security, privacy, and lawful use of data as explain in figure 2 (Savola *et al.*, 2020). Cloud providers and organizations using these platforms must navigate a complex landscape of global, regional, and industry-specific standards to safeguard data integrity and uphold privacy (Vashishth *et al.*, 2023). A robust compliance framework that encompasses data residency, audit requirements, and vendor compliance helps organizations align with regulatory obligations and mitigate legal risks associated with cloud data management.

Compliance with global and regional standards is fundamental for organizations that store or process data in the cloud. Key regulations, such as the General Data Protection Regulation (GDPR) in the European Union, mandate strict guidelines for data privacy, security, and the handling of personal data. GDPR's principles on data processing, user consent, and the "right to be forgotten" have become benchmarks for cloud data governance, affecting organizations globally that serve EU customers (Mangini *et al.*, 2020). In the United States, the Health Insurance Portability and Accountability Act (HIPAA) mandates strict privacy and security measures for healthcare data. Similarly, the California Consumer Privacy Act (CCPA) imposes rules on data transparency and consumer rights for businesses operating in California. These standards require cloud service providers and their clients to establish strong data protection protocols, ensuring that personal and sensitive information is securely managed (Gupta *et al.*, 2022). For organizations operating internationally, navigating these varying compliance standards is critical, as non-compliance can result in hefty fines and reputational damage.

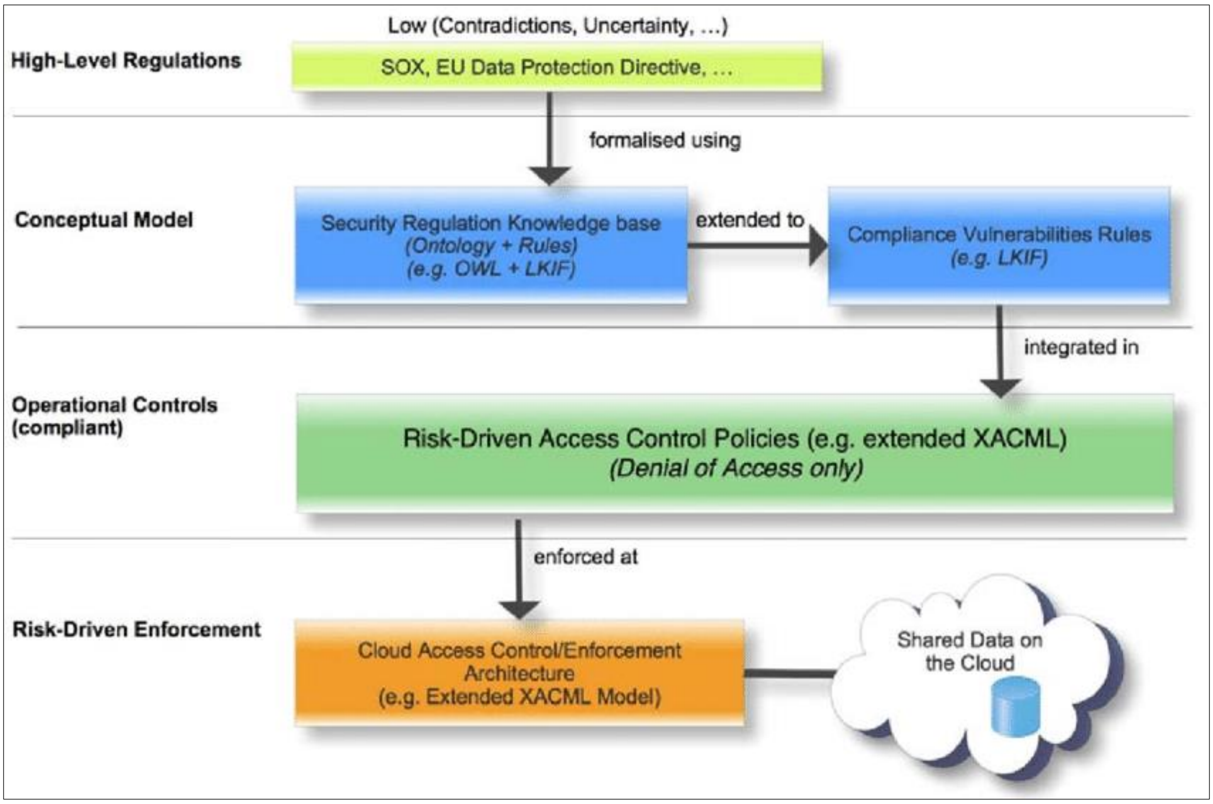

Low (Contradictions, Uncertainty, ...)
High-Level Regulations
SOX, EU Data Protection Directive, ...
formalised using
Conceptual Model
Security Regulation Knowledge base (Ontology + Rules) (e.g. OWL + LKIF)
extended to
Compliance Vulnerabilities Rules (e.g. LKIF)
integrated in
Operational Controls (compliant)
Risk-Driven Access Control Policies (e.g. extended XACML) (Denial of Access only)
enforced at
Risk-Driven Enforcement
Cloud Access Control/Enforcement Architecture (e.g. Extended XACML Model)
Shared Data on the Cloud

Figure 2 A Plan to Implement Compliant Access Control (Savola *et al.*, 2020)

Data residency and sovereignty policies dictate where data can be stored and processed, often driven by concerns about data privacy and national security. These policies are crucial for cloud environments, where data may be dispersed across global data centers. Some regulations require that data originating within a specific region, such as the European Union or China, remain within that region, creating challenges for global cloud deployments (Choi, 2022). To address this, cloud providers often offer data localization options that allow organizations to choose specific data centers for data storage. This ensures that data complies with local laws, minimizing risks associated with cross-border data transfers. Additionally, cloud providers and organizations must carefully manage cross-border data flows, particularly when transferring data between regions with differing regulations. Compliance with data residency requirements helps organizations mitigate regulatory risks, adhere to sovereignty laws, and maintain customer trust by respecting data location preferences.

Compliance frameworks typically require rigorous documentation, reporting, and audit mechanisms to demonstrate regulatory adherence. Audits and reporting play a significant role in cloud environments, where transparency is essential for monitoring data access, ensuring policy compliance, and managing security incidents. Regular audits, both internal and third-party, allow organizations to assess their compliance posture and identify areas for improvement. Compliance documentation, such as data processing agreements and access logs, is essential for proving adherence to regulations like GDPR and HIPAA (Ahmad and Salleh, 2021). Cloud providers also frequently undergo independent audits to certify their compliance with standards such as SOC 2, ISO 27001, and FedRAMP, providing their clients with additional assurance. Reporting requirements further necessitate prompt disclosure of data breaches or security incidents, aligning cloud providers and clients with regulatory expectations for transparency and accountability. By maintaining comprehensive audit trails and reporting practices, organizations can ensure regulatory compliance and foster a culture of accountability in cloud data management.

Ensuring that vendors and third-party providers align with compliance requirements is critical, as cloud ecosystems often involve multiple parties that manage or access sensitive data. Third-party compliance requires that all parties involved in data handling or processing uphold the same standards of security, privacy, and transparency (Georgiopoulou *et al*., 2020). Many organizations use standardized contractual agreements, such as Data Processing Agreements (DPAs), to enforce compliance requirements across third-party vendors. These agreements specify security measures, data handling practices, and accountability for breaches or compliance failures. Additionally, vendor assessments and due diligence practices help organizations evaluate third-party compliance capabilities before engaging with them. Continuous monitoring of third-party compliance ensures that cloud providers and partners adhere to the relevant regulatory standards, protecting the organization's data and minimizing exposure to compliance risks (Khalil, 2020; Haber *et al*., 2022).

Compliance and regulatory policies are foundational to managing data securely and lawfully in cloud computing environments (Stephen and Smith, 2022). Adhering to global and regional standards such as GDPR and HIPAA, implementing data residency and sovereignty controls, fulfilling audit and reporting obligations, and enforcing vendor compliance are essential components of a robust compliance framework. Together, these policies help organizations navigate the complex regulatory landscape, safeguard data, and uphold privacy and transparency in cloud environments. As regulations continue to evolve, maintaining adaptability and proactive compliance practices will remain vital for organizations seeking to leverage cloud computing while minimizing legal and operational risks.

2.3. Cloud Management Policies

Cloud management policies are essential for organizations to effectively control cloud resources, optimize costs, and ensure that services meet operational needs and business goals as a means of data storage as explain in figure 3 (Seth *et al*., 2022). As cloud infrastructure grows more complex, establishing policies for resource allocation, service-level agreements (SLAs), disaster recovery, and performance monitoring provides a structured approach to managing cloud resources (Girs *et al*., 2020; Prasad *et al*., 2023). These policies allow organizations to efficiently utilize cloud services, maintain operational continuity, and enhance service resilience.

Effective resource allocation and cost management are fundamental in cloud environments where services are charged on a pay-as-you-go basis. Policies for resource allocation involve setting guidelines for distributing computational resources, storage, and network bandwidth based on application requirements and organizational priorities. Organizations should implement cost-tracking measures, such as automated tagging of resources by department or project, to accurately monitor and allocate expenses (Dastres *et al*., 2022). Additionally, cost management policies often include setting budget limits, utilizing cost forecasting tools, and implementing usage alerts to prevent unforeseen expenses. Cost-effective resource usage also requires regular optimization of resource allocation by shutting down unused resources, consolidating workloads, and leveraging reserved instances or spot instances for predictable workloads. By enforcing strict policies on resource allocation and cost tracking, organizations can optimize spending, prevent budget overruns, and maximize return on investment in cloud infrastructure.

Service Level Agreements (SLAs) are critical for establishing expectations regarding the performance, availability, and support provided by cloud service providers. SLAs define the minimum acceptable standards for service uptime, data availability, latency, and response times, giving organizations a basis for evaluating service quality (Qureshi *et al*., 2020). For instance, an SLA might specify that a cloud service will have 99.9% uptime, meaning that downtime is limited to 43 minutes per month. SLAs also outline compensation terms for any service disruptions that fail to meet agreed standards, such as service credits or financial reimbursement. Establishing clear SLAs helps organizations assess whether cloud services align with their business needs, providing assurance of reliability and holding providers accountable. Organizations can further protect themselves by including clauses that address data access rights, termination conditions, and security compliance. Regularly reviewing SLAs ensures that cloud services continue to meet operational requirements as workloads evolve, maintaining service continuity and performance (Tawfeeg *et al.*, 2022).

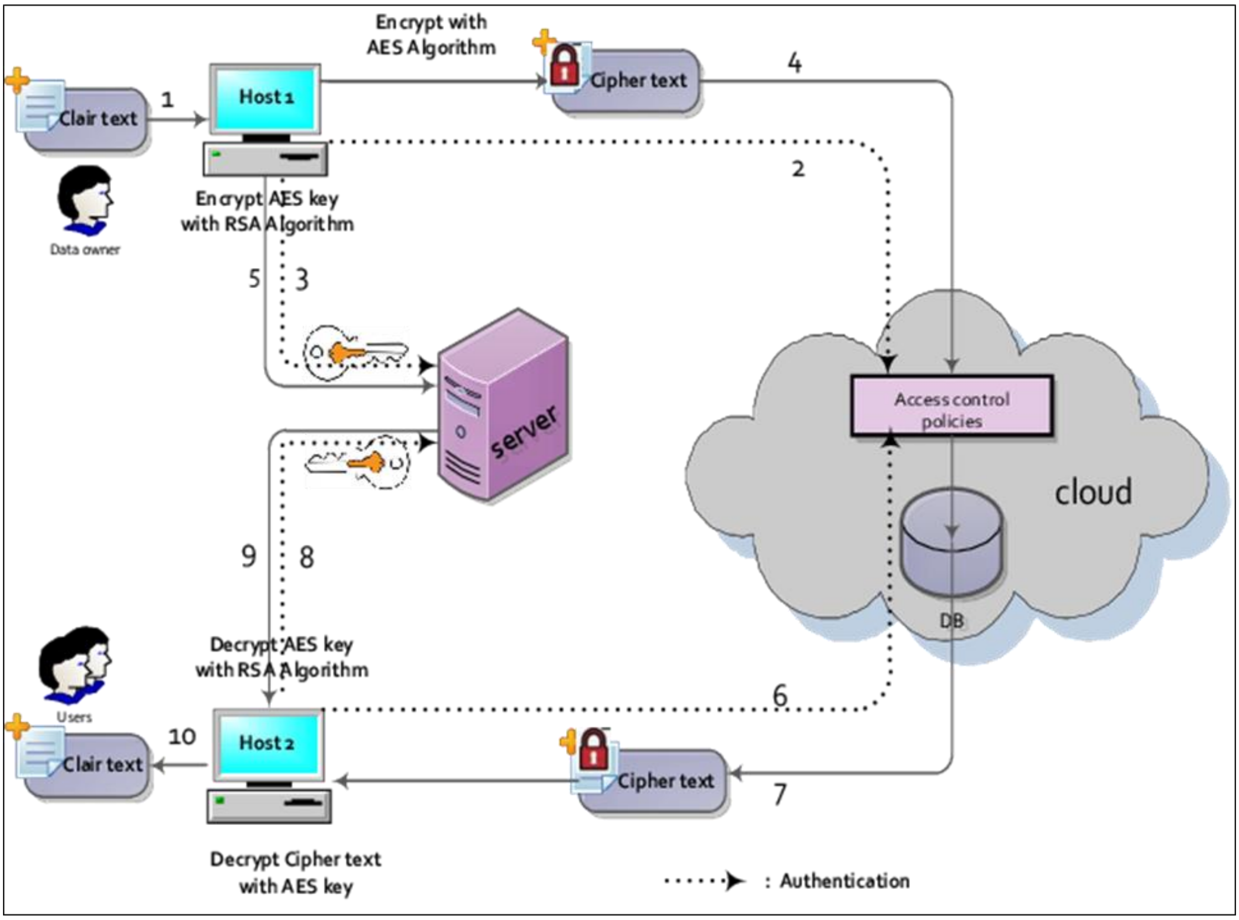


Figure 3 Cloud computing data storage approach that has been proposed (Seth *et al.*, 2022)

Disaster recovery and business continuity policies are essential for safeguarding data and ensuring rapid recovery following disruptions. Cloud environments require a disaster recovery plan (DRP) that outlines the steps for data backup, restoration, and failover procedures in the event of system failures, cyberattacks, or natural disasters (Bhardwaj *et al.*, 2022). Key components of a DRP include data replication across multiple geographic regions, regular backup schedules, and automated failover mechanisms. Business continuity policies extend disaster recovery by specifying procedures to maintain critical operations during downtime, ensuring minimal disruption to business functions. These policies also address recovery time objectives (RTOs) and recovery point objectives (RPOs), which define acceptable limits for downtime and data loss, respectively. For instance, an RTO of four hours and an RPO of one hour might mean that services should be restored within four hours, with data no more than one hour old. By establishing robust disaster recovery and business continuity policies, organizations can enhance resilience, reduce recovery times, and maintain operational stability even during unexpected disruptions (Suresh *et al.*, 2020).

Performance and capacity monitoring policies are crucial to ensuring that cloud resources meet demand and perform optimally. Cloud environments can experience fluctuating workloads, making it essential to regularly assess and scale resources to accommodate peak demand (Muhammad, 2022). Policies for performance monitoring involve tracking metrics such as CPU and memory usage, storage capacity, latency, and application response times. Automated alerts can notify administrators when performance metrics reach critical thresholds, allowing for proactive scaling or reallocation of resources. Capacity planning policies, on the other hand, help organizations anticipate future demand based on historical usage data, enabling the pre-allocation of resources during high-demand periods. For instance, an e-commerce platform may need to increase capacity during holiday seasons to handle increased traffic. By implementing performance and capacity monitoring policies, organizations can maintain optimal service levels, avoid performance bottlenecks, and ensure that resources are allocated in a way that supports user needs without overspending.

Cloud management policies provide a framework for efficient resource utilization, service reliability, disaster recovery, and performance optimization in cloud computing environments (Abualkishik *et al*., 2020). By defining policies for resource allocation and cost management, organizations can optimize their cloud expenditures and allocate resources efficiently. SLAs establish clear expectations for service quality and reliability, ensuring that cloud services align with business needs. Disaster recovery and business continuity policies further strengthen operational resilience, allowing organizations to quickly recover from unexpected disruptions. Finally, performance and capacity monitoring policies enable proactive scaling to meet demand, maintaining high service levels. As cloud adoption continues to grow, these management policies will remain essential in enabling organizations to maximize the value of cloud investments while maintaining stability, security, and operational efficiency.

2.4. Challenges and Limitations in Cloud Computing Policy Frameworks

The rapid adoption of cloud computing has brought numerous benefits to organizations, including scalability, cost savings, and advanced analytics (Golightly *et al*., 2022). However, it also presents several challenges and limitations, especially as organizations implement policies for multi-cloud and hybrid environments, adapt to technological changes, and safeguard data security and privacy. Addressing these challenges is critical for organizations to maximize the benefits of cloud technology while mitigating associated risks.

One significant challenge in cloud computing is managing the complexity of multi-cloud and hybrid environments. Many organizations now use services from multiple cloud providers, or a mix of on-premises and cloud-based resources, to meet their specific needs (Zhang and Yue, 2020). While this approach offers flexibility and can reduce dependency on a single provider, it also introduces challenges in policy consistency, interoperability, and integration. Each cloud platform has its own unique set of services, interfaces, and compliance protocols, which can lead to fragmented policies and inconsistencies in governance and data management. Ensuring policy alignment across these diverse environments requires sophisticated orchestration and monitoring tools that provide a unified view of operations across platforms. This complexity can slow down policy implementation and introduce additional operational risks if not properly managed, as different environments may have varying levels of compliance or security controls. Thus, organizations must invest in robust management solutions and expertise to address these challenges, ensuring a cohesive approach to policy enforcement in multi-cloud and hybrid setups.

The speed at which cloud and AI technologies evolve poses another challenge for policy frameworks (Dwivedi *et al*., 2021). Emerging technologies, including AI-driven analytics, automation, and machine learning, continuously redefine how cloud services are deployed, managed, and secured. This rapid advancement makes it difficult to establish long-term policies, as guidelines can quickly become outdated or irrelevant. Policies for data security, compliance, and resource allocation must remain adaptable to incorporate new features or tools offered by cloud providers. For instance, the introduction of AI-based predictive analytics can improve resource allocation, but existing policies may not account for the potential risks or resource demands of these tools. Moreover, regulatory frameworks themselves are continuously evolving in response to technological advancements, requiring organizations to frequently update their policies to stay compliant (Brass and Sowell, 2021). To keep pace, organizations should adopt agile approaches to policy development, where policies are designed to be reviewed and modified regularly, incorporating the latest industry standards and technological capabilities.

Data security and privacy remain central concerns in cloud computing, especially as data is increasingly distributed across cloud platforms and accessed remotely (Akhtar *et al*., 2021). The accessibility and scalability of cloud computing can introduce vulnerabilities that traditional on-premises systems may not have, such as unauthorized access, data leaks, and cyberattacks. Organizations must strike a balance between making data easily accessible for legitimate users while implementing stringent security controls to protect sensitive information. Policies must address identity and access management (IAM), encryption, and incident response protocols to mitigate these risks. However, ensuring robust data security while maintaining cloud accessibility is often challenging, as stricter security measures can sometimes limit functionality or impact user experience. Additionally, compliance with privacy regulations, such as GDPR or CCPA, imposes stringent requirements on data handling, storage, and access. Failure to protect data effectively not only leads to potential regulatory penalties but also damages an organization’s reputation. Therefore, comprehensive security policies, regular security audits, and training on best practices for cloud security are essential to safeguarding data without compromising accessibility (Ismail and Islam, 2020).

The adoption of cloud computing offers numerous benefits, but challenges and limitations need to be carefully managed to ensure its effective and secure use. The complexity of multi-cloud and hybrid environments requires organizations to develop strategies for consistent policy enforcement across diverse platforms. Rapid technological changes in AI and cloud computing demand flexible and adaptable policies, while the ever-present risks to data security and privacy necessitate stringent, up-to-date security measures (Silva and Soto, 2022). By addressing these challenges, organizations can create a policy framework that not only optimizes cloud resources but also maintains compliance, enhances security, and supports long-term growth. As cloud computing technology continues to evolve, these challenges will persist, making it essential for organizations to invest in continuous policy review and update processes to keep pace with technological advancements and regulatory requirements.

2.5. Future Directions in Cloud Computing Policy Frameworks

As cloud computing and artificial intelligence (AI) continue to grow, policy frameworks must evolve to address emerging challenges and leverage new opportunities (Cowls *et al*., 2023). Future directions in cloud computing policies will focus on adapting to AI advancements, integrating emerging regulations, and fostering collaborative policy development. These trends will shape the landscape of cloud governance, security, and compliance, guiding organizations in responsible and effective cloud adoption.

The evolution of AI in cloud computing brings both immense potential and unique challenges, driving the need for more sophisticated policy frameworks. AI-powered cloud services offer capabilities such as predictive analytics, intelligent automation, and advanced cybersecurity, transforming business operations (Reddy, 2022). However, the integration of AI into cloud computing requires policies that address issues such as ethical AI use, transparency, accountability, and the management of AI models across their lifecycle. Future policy frameworks are likely to include standardized guidelines for AI ethics, ensuring AI systems are fair, transparent, and free from bias. Moreover, as AI algorithms become more complex, policies must also govern the data used for training these models to prevent unethical or biased outcomes. To manage the rapid pace of AI advancements, policymakers may adopt agile policy approaches that allow for quick revisions and updates, ensuring policies remain relevant and effective. Additionally, these policies will need to prioritize AI explainability and model interpretability to help organizations maintain trust in AI-based cloud services and meet regulatory requirements.

With the global regulatory environment becoming increasingly complex, cloud computing policies will need to adapt to new and forthcoming data protection and privacy laws (Abdulsalam and Hedabou, 2021). Regulations such as the European Union's General Data Protection Regulation (GDPR) have set high standards for data security and privacy, and similar frameworks are emerging worldwide. For instance, countries like Brazil (LGPD), India (Data Protection Bill), and the United States (various state-level regulations like the California Consumer Privacy Act) are introducing or refining data protection laws that impact cloud services. These laws require organizations to comply with strict data handling, storage, and transfer standards, especially in cross-border data exchanges. The trend of data residency requirements where data must remain within specific geographic boundaries—further complicates cloud policy frameworks, as organizations must navigate different laws across regions. Cloud providers and their customers will need to establish policies that address data localization, data portability, and compliance documentation (Saini *et al*., 2022). Future regulatory trends will likely focus on expanding these protections, and global organizations must remain adaptable to comply with new mandates. Compliance with these regulations will require organizations to implement robust data governance frameworks, reinforcing cloud policies with automated compliance monitoring and continuous auditing.

The complexity of cloud and AI policy challenges necessitates collaborative development efforts among industry stakeholders, including cloud providers, regulatory bodies, industry associations, and user organizations. Collaboration can help create comprehensive, standardized frameworks that reduce ambiguity and foster widespread adoption of best practices (Chowdhury *et al*., 2022). Industry-wide cooperation enables policymakers to draw from diverse perspectives, ensuring policies are not only compliant with regulatory standards but also feasible for practical implementation. Collaborative frameworks can standardize approaches to critical issues like data privacy, AI ethics, and cybersecurity, allowing organizations to align with widely accepted norms. Initiatives such as the Cloud Security Alliance (CSA) and OpenAI's ethical guidelines represent early examples of industry-driven collaboration in addressing cloud and AI policy issues. Moving forward, multi-stakeholder partnerships will play an increasingly important role in defining guidelines for complex issues like cross-border data transfers, AI transparency, and model accountability (Pisa *et al*., 2020). By developing cohesive policies that incorporate best practices, organizations can enhance interoperability, streamline compliance efforts, and build consumer trust in cloud services.

Future policy frameworks for cloud computing will need to keep pace with technological advancements in AI, respond to evolving regulatory landscapes, and benefit from industry collaboration. Evolving AI capabilities will require dynamic policies that balance innovation with ethical considerations, ensuring AI systems are transparent, accountable, and fair. Emerging regulations will continue to shape global data governance practices, compelling organizations to adapt policies for data sovereignty, compliance documentation, and privacy protection (Arner *et al*., 2022). Collaborative policy development will be essential for creating effective, standardized frameworks that address these challenges comprehensively and facilitate best practices across the industry. As cloud computing and AI technologies continue to advance, organizations that proactively embrace these future policy directions will be better positioned to navigate regulatory requirements, maintain robust governance, and foster sustainable innovation. Through continuous adaptation, cloud policy frameworks can support the responsible growth of cloud and AI technologies, benefiting businesses and users alike (Robertson *et al*., 2021).

3. Conclusion

In summary, a comprehensive policy framework for cloud computing is crucial in guiding organizations through the complex terrain of AI integration, governance, compliance, and management. Robust policies around AI focus on ethics, accountability, and fairness, ensuring AI systems operate transparently and responsibly within cloud environments. Governance frameworks emphasize clear roles, data stewardship, and continuous risk management, supporting efficient, secure cloud operations. Compliance policies address diverse regulatory requirements, data sovereignty, and audit readiness, while cloud management strategies ensure cost-effective resource allocation, SLAs, disaster recovery, and performance monitoring.

The importance of such policies cannot be overstated, as they underpin the security, reliability, and regulatory alignment of cloud operations. As organizations increasingly rely on cloud services, comprehensive policies are essential to mitigate risks, safeguard data, and optimize performance. Effective policy frameworks create a foundation for ethical and efficient use of cloud-based AI, while also meeting the demands of rapidly changing compliance landscapes. By ensuring alignment with industry best practices and regulatory standards, robust cloud policies enhance organizational resilience and adaptability.

To implement a strong cloud policy framework, organizations should first prioritize collaboration between IT, compliance, and management teams to ensure a holistic approach. Regular policy reviews and updates are essential to accommodate emerging technologies and regulations. Investing in monitoring and auditing tools can further streamline compliance and governance practices, while fostering a culture of accountability. By taking these steps, organizations can build a policy framework that not only strengthens cloud security and compliance but also empowers them to leverage cloud technology's full potential responsibly and effectively. This proactive approach will be essential as cloud computing continues to evolve, ensuring sustainable growth and innovation in the digital landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Benlian, A., Kettinger, W.J., Sunyaev, A., Winkler, T.J. and Guest Editors, 2018. The transformative value of cloud computing: a decoupling, platformization, and recombination theoretical framework. *Journal of management information systems*, *35*(3), pp.719-739.

[2] Bello, S.A., Oyedele, L.O., Akinade, O.O., Bilal, M., Delgado, J.M.D., Akanbi, L.A., Ajayi, A.O. and Owolabi, H.A., 2021. Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, p.103441.

[3] Kommisetty, P.D.N.K., 2022. Leading the Future: Big Data Solutions, Cloud Migration, and AI-Driven Decision-Making in Modern Enterprises. *Educational Administration: Theory and Practice*, *28*(03), pp.352-364.

[4] Kumar, B., 2022. Challenges and Solutions for Integrating AI with Multi-Cloud Architectures. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *1*(1), pp.71-77.

[5] Benson, V., Furnell, S., Masi, D. and Muller, T., 2021. Regulation, Policy and Cybersecurity.

[6] Mahajan, V., 2023. From Compliance to Cost Optimization: AI's Role in Modern Cloud Security Strategies. *Journal of Artificial Intelligence Research*, *3*(1), pp.239-275.

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

[8] Kanungo, S., 2020. REVOLUTIONIZING DATA PROCESSING: ADVANCED CLOUD COMPUTING AND AI SYNERGY FOR IOT INNOVATION. *International Research Journal of Modernization in Engineering Technology and Science*, *2*, pp.1032-1040.

[9] Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J. and Al-Fuqaha, A., 2022. Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, p.100452.

[10] Kavitha, S., Bora, A., Naved, M., Raj, K.B. and Singh, B.R.N., 2021. An internet of things for data security in cloud using artificial intelligence. *International Journal of Grid and Distributed Computing*, *14*(1), pp.1257-1275.

[11] Hardt, M., Chen, X., Cheng, X., Donini, M., Gelman, J., Gollaprolu, S., He, J., Larroy, P., Liu, X., McCarthy, N. and Rathi, A., 2021, August. Amazon sagemaker clarify: Machine learning bias detection and explainability in the cloud. In *Proceedings of the 27th ACM SIGKDD conference on knowledge discovery and data mining* (pp. 2974-2983).

[12] Perifanis, N.A. and Kitsios, F., 2022. Edge and fog computing business value streams through IoT solutions: A literature review for strategic implementation. *Information*, *13*(9), p.427.

[13] Kaur, D., Uslu, S., Rittichier, K.J. and Durresi, A., 2022. Trustworthy artificial intelligence: a review. *ACM computing surveys (CSUR)*, *55*(2), pp.1-38.

[14] Wohlrab, R., Knauss, E., Steghöfer, J.P., Maro, S., Anjorin, A. and Pelliccione, P., 2020. Collaborative traceability management: a multiple case study from the perspectives of organization, process, and culture. *Requirements Engineering*, *25*(1), pp.21-45.

[15] Machireddy, J.R., Rachakatla, S.K. and Ravichandran, P., 2021. Leveraging AI and Machine Learning for Data-Driven Business Strategy: A Comprehensive Framework for Analytics Integration. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), pp.12-150.

[16] Shah, V. and Konda, S.R., 2022. Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. *Revista Espanola de Documentacion Cientifica*, *16*(3), pp.50-71.

[17] Jaatun, M.G., Pearson, S., Gittler, F., Leenes, R. and Niezen, M., 2020. Enhancing accountability in the cloud. *International Journal of Information Management*, *53*, p.101498.

[18] Manohar, S., Kapoor, A. and Ramesh, A., 2020. Understanding data stewardship: taxonomy and use cases. *Last accessed on October*, *15*, p.2022.

[19] Stein, M., Campitelli, V. and Mezzio, S., 2020. Managing the impact of cloud computing. *CPA Journal*, *90*(6).

[20] Torkura, K.A., Sukmana, M.I., Cheng, F. and Meinel, C., 2021. Continuous auditing and threat detection in multi-cloud infrastructure. *Computers and Security*, *102*, p.102124.

[21] Dittakavi, R.S.S., 2022. Evaluating the efficiency and limitations of configuration strategies in hybrid cloud environments. *International Journal of Intelligent Automation and Computing*, *5*(2), pp.29-45.

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

[23] Cardoni, A., Kiseleva, E. and De Luca, F., 2020. Continuous auditing and data mining for strategic risk control and anticorruption: Creating "fair" value in the digital age. *Business Strategy and the Environment*, *29*(8), pp.3072-3085.

[24] Vashishth, T.K., Sharma, V., Kumar, B. and Sharma, K.K., 2023. Cloud-Based Data Management for Behavior Analytics in Business and Finance Sectors. In *Data-Driven Modelling and Predictive Analytics in Business and Finance* (pp. 133-155). Auerbach Publications.

[25] Gupta, I., Singh, A.K., Lee, C.N. and Buyya, R., 2022. Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEE Access*, *10*, pp.71247-71277.

[26] Choi, Y.J., 2022. Corporate social responsibility. In *Encyclopedia of Big Data* (pp. 220-223). Cham: Springer International Publishing.

[27] Ahmad, H. and Salleh, L., 2021. Ensuring Data Integrity in Large-Scale Migration Projects. *Sage Science Review of Educational Technology*, *4*(2), pp.69-92.

[28] Georgiopoulou, Z., Makri, E.L. and Lambrinoudakis, C., 2020. GDPR compliance: proposed technical and organizational measures for cloud provider. *Information and Computer Security*, *28*(5), pp.665-680.

[29] Haber, M.J., Chappell, B. and Hills, C., 2022. Regulatory compliance. In *Cloud Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Cloud Resources* (pp. 297-373). Berkeley, CA: Apress.

[30] Stephen, M. and Smith, L., 2022. Evaluating Encryption Techniques in Cloud Computing for Enhanced Data Privacy.

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

[32] Prasad, V.K., Dansana, D., Bhavsar, M.D., Acharya, B., Gerogiannis, V.C. and Kanavos, A., 2023. Efficient Resource Utilization in IoT and Cloud Computing. *Information*, *14*(11), p.619.

[33] Girs, S., Sentilles, S., Asadollah, S.A., Ashjaei, M. and Mubeen, S., 2020. A systematic literature study on definition and modeling of service-level agreements for cloud services in IoT. *IEEE Access*, *8*, pp.134498-134513.

[34] Dastres, R., Soori, M. and Asamel, M., 2022. Radio Frequency Identification (RFID) based wireless manufacturing systems, a review. *Independent Journal of Management and Production*, *13*(1), pp.258-290.

[35] Qureshi, H.N., Manalastas, M., Zaidi, S.M.A., Imran, A. and Al Kalaa, M.O., 2020. Service level agreements for 5G and beyond: overview, challenges and enablers of 5G-healthcare systems. *Ieee Access*, *9*, pp.1044-1061.

[36] Tawfeeg, T.M., Yousif, A., Hassan, A., Alqhtani, S.M., Hamza, R., Bashir, M.B. and Ali, A., 2022. Cloud dynamic load balancing and reactive fault tolerance techniques: a systematic literature review (SLR). *IEEE Access*, *10*, pp.71853-71873.

[37] Bhardwaj, P., Lohani, K., Tomar, R. and Srivastava, R., 2022. Comparative analysis of traditional and cloud-based disaster recovery methods. In *Intelligent Computing Techniques for Smart Energy Systems: Proceedings of ICTSES 2021* (pp. 105-117). Singapore: Springer Nature Singapore.

[38] Suresh, N.C., Sanders, G.L. and Braunscheidel, M.J., 2020. Business continuity management for supply chains facing catastrophic events. *IEEE Engineering Management Review*, *48*(3), pp.129-138.

[39] Muhammad, T., 2022. A Comprehensive Study on Software-Defined Load Balancers: Architectural Flexibility and Application Service Delivery in On-Premises Ecosystems. *International Journal of Computer Science and Technology*, *6*(1), pp.1-24.

[40] Abualkishik, A.Z., Alwan, A.A. and Gulzar, Y., 2020. Disaster recovery in cloud computing systems: An overview. *International Journal of Advanced Computer Science and Applications*, *11*(9).

[41] Golightly, L., Chang, V., Xu, Q.A., Gao, X. and Liu, B.S., 2022. Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, *14*, p.18479790221093992.

[42] Zhang, X. and Yue, W.T., 2020. Integration of on-premises and cloud-based software: the product bundling perspective. *Journal of the Association for Information Systems*, *21*(6), p.6.

[43] Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A. and Galanos, V., 2021. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, *57*, p.101994.

[44] Brass, I. and Sowell, J.H., 2021. Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation and Governance*, *15*(4), pp.1092-1110.

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

[46] Ismail, U.M. and Islam, S., 2020. A unified framework for cloud security transparency and audit. *Journal of information security and applications*, *54*, p.102594.

[47] Silva, I. and Soto, M., 2022. Privacy-preserving data sharing in healthcare: an in-depth analysis of big data solutions and regulatory compliance. *International Journal of Applied Health Care Analytics*, *7*(1), pp.14-23.

[48] Cowls, J., Tsamados, A., Taddeo, M. and Floridi, L., 2023. The AI gambit: leveraging artificial intelligence to combat climate change—opportunities, challenges, and recommendations. *Ai and Society*, pp.1-25.

[49] Reddy, A.R.P., 2022. The Future of Cloud Security: Ai-Powered Threat Intelligence and Response. *International Neurourology Journal*, *26*(4), pp.45-52.

[50] Abdulsalam, Y.S. and Hedabou, M., 2021. Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), p.11.

[51] Saini, J.S., Saini, D.K., Gupta, P., Lamba, C.S. and Rao, G.M., 2022. [Retracted] Cloud Computing: Legal Issues and Provision. *Security and Communication Networks*, *2022*(1), p.2288961.

[52] Chowdhury, S., Budhwar, P., Dey, P.K., Joel-Edgar, S. and Abadie, A., 2022. AI-employee collaboration and business performance: Integrating knowledge-based view, socio-technical systems and organisational socialisation framework. *Journal of Business Research*, *144*, pp.31-49.

[53] Pisa, M., Dixon, P., Ndulu, B. and Nwankwo, U., 2020. Governing data for development: trends, challenges, and opportunities. *CGD Policy Paper*, *190*, pp.1-61.

[54] Arner, D.W., Castellano, G.G. and Selga, E.K., 2022. The transnational data governance problem. *Berkeley Tech. LJ*, *37*, p.623.

[55] Robertson, J., Fossaceca, J.M. and Bennett, K.W., 2021. A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations. *IEEE Transactions on Engineering Management*, *69*(6), pp.3913-3922.

[56] Dondapati, A., Sheoliha, N., Panduro-Ramirez, J., Bakhare, R., Sreejith, P.M. and Kotni, V.D.P., 2022. An integrated artificial intelligence framework for knowledge production and B2B marketing rational analysis for enhancing business performance. *Materials Today: Proceedings*, *56*, pp.2232-2235.

[57] Savola, R.M., Kylänpää, M. and Abie, H., 2020. Risk-driven security metrics for an Android smartphone application. *International Journal of Electronic Business*, *15*(4), pp.297-324.

[58] Seth, B., Dalal, S., Jaglan, V., Le, D.N., Mohan, S. and Srivastava, G., 2022. Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, *33*(4), p.e4108.

[59] Mangini, V., Tal, I. and Moldovan, A.N., 2020, August. An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-9).

[60] Saraswat, M. and Tripathi, R.C., 2020, December. Cloud computing: Analysis of top 5 CSPs in SaaS, PaaS and IaaS platforms. In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)* (pp. 300-305). IEEE.