World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

A comprehensive model for ensuring data compliance in cloud computing environment

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

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

World Journal of Advanced Research and Reviews, 2024, 24(02), 1983–1995

Publication history: Received on 07 October 2024; revised on 17 November 2024; accepted on 20 November 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.2.3514

Abstract

As organizations increasingly adopt cloud computing, ensuring data compliance has become a critical priority. Cloud environments pose unique challenges in meeting regulatory requirements due to their distributed and often multi-tenant nature. This review presents a comprehensive model for achieving data compliance in cloud computing, addressing essential aspects such as data privacy, security, sovereignty, and governance. The model emphasizes a structured, layered approach to compliance, integrating risk assessment, data governance, continuous monitoring, and incident management to ensure compliance throughout the data lifecycle. Key components of the proposed model include robust data privacy and protection mechanisms aligned with global regulations such as GDPR and CCPA, data security protocols for safeguarding confidentiality and access control, and data sovereignty policies to handle jurisdictional requirements and cross-border data flows. Additionally, continuous monitoring and automated auditing tools enhance real-time compliance management, while incident management procedures prepare organizations to respond promptly to breaches or policy violations. The framework also incorporates advanced technological solutions, including compliance automation, data loss prevention, and blockchain for traceability, to streamline compliance tasks and improve transparency. By addressing both the technical and governance aspects of data compliance, this model supports organizations in navigating complex regulatory landscapes across multi-cloud and hybrid environments. The review highlights best practices for ensuring compliance, such as regular policy updates, employee training, and third-party compliance management, to sustain long-term adherence. As the regulatory landscape evolves and new privacy-preserving technologies emerge, this model offers a scalable and adaptive approach, positioning organizations to manage data compliance effectively within dynamic cloud infrastructures. This comprehensive approach ensures secure, compliant data operations, fostering trust and accountability in cloud computing environments.

Keywords: Data Compliance; Cloud Computing; Environment; Comprehensive Model

1. Introduction

Data compliance in cloud computing has emerged as a critical concern for organizations navigating the complexities of managing sensitive information in a digital environment (Tabrizchi and Kuchaki, 2020). With the rapid adoption of cloud technologies, the storage and processing of vast amounts of data are often decentralized across multiple jurisdictions. This proliferation raises significant challenges related to regulatory compliance, data privacy, and security. Various compliance frameworks exist, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, each imposing stringent requirements on how data is handled, stored, and transferred (Carlson *et al*al., 2020; Lancieri, 2022). Failure to comply can result in severe penalties,

[*] Corresponding author: Adebola Folorunso

reputational damage, and loss of consumer trust. Consequently, organizations are compelled to implement robust data compliance strategies that align with the evolving regulatory landscape while ensuring the security of their data assets (Muhammad *et al*al., 2022).

A comprehensive model for data compliance is essential in this context. Such a model provides a structured framework that enables organizations to systematically address compliance obligations across diverse cloud environments. By integrating best practices from various regulatory requirements, a comprehensive model facilitates the alignment of organizational policies with legal mandates, promoting consistency and accountability in data handling (Shneiderman, 2020; Huising and Silbey, 2021). It not only serves as a guideline for achieving compliance but also helps organizations to identify potential risks and gaps in their data governance frameworks. Furthermore, a well-defined compliance model fosters a culture of transparency and ethical data use, enhancing stakeholder confidence and driving organizational success in the digital economy (Shepherd *et al*al., 2002).

The objectives of this review are twofold: first, to define a structured approach that ensures compliance across cloud environments, and second, to outline the key components of a comprehensive compliance model that organizations can adopt. This structured approach will encompass several critical areas, including data governance, risk management, and the integration of compliance technologies. By adopting such a model, organizations can effectively navigate the complexities of cloud compliance, ensuring that their operations adhere to both local and international regulations. Ultimately, the establishment of a comprehensive model for data compliance will not only safeguard organizational interests but also contribute to the broader goal of fostering responsible and ethical practices in cloud computing (Ahsan and Shabbir, 2021; Srivastava and Bag, 2023). This foundational understanding sets the stage for a deeper exploration of the challenges and strategies associated with achieving data compliance in cloud environments.

2. Components of Data Compliance in Cloud Computing

Data compliance in cloud computing encompasses various components that organizations must consider to ensure the secure and lawful handling of sensitive information as explain in figure 1 (Ahmad *et al*al., 2021; Parast *et al*al., 2022). 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.

Data privacy laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States have profound implications for cloud computing (Hartzog and Richards, 2020; Yanamala and Suryadevara, 2023). These regulations establish strict guidelines for how personal data must be collected, processed, and stored, imposing significant responsibilities on organizations that utilize cloud services. Under these laws, data privacy principles such as data minimization, purpose limitation, and user consent are paramount. Data minimization mandates that organizations only collect data that is necessary for the intended purpose, thereby reducing the risk of overexposure and misuse. Purpose limitation requires organizations to clearly define and communicate the specific purposes for which data is collected, preventing unauthorized or ambiguous uses. User consent is a critical element that empowers individuals by allowing them to control how their data is utilized, fostering transparency and trust (Segijn *et al*al., 2021). Collectively, these principles emphasize the importance of respecting user privacy and aligning data handling practices with legal requirements.

The integrity of data in cloud computing is intrinsically linked to security measures. Organizations must implement robust security protocols, including encryption, access controls, and secure data transfer methods (Patil *et al*al., 2021). Encryption ensures that data is rendered unreadable to unauthorized users, protecting sensitive information from potential breaches during storage and transit. Access controls further enhance security by restricting data access to authorized personnel, thereby minimizing the risk of insider threats and external attacks. Additionally, multi-factor authentication (MFA) and identity management play critical roles in safeguarding sensitive data. MFA requires users to provide multiple forms of verification before accessing cloud services, significantly enhancing security. Identity management systems help organizations effectively manage user identities and permissions, ensuring that only those with the requisite authority can access sensitive data (Sung and Park, 2021). Together, these measures create a layered security approach that reinforces data confidentiality.

As organizations increasingly adopt multi-cloud and hybrid environments, data sovereignty and localization regulations become crucial. Data residency laws mandate that certain data be stored within specific geographic boundaries, often due to legal and regulatory requirements (Lukings and Habibi, 2022). Compliance with these regulations necessitates a thorough understanding of jurisdictional requirements and the implications for data movement across borders.

Managing data residency in multi-cloud environments presents unique challenges. Organizations must develop strategies that balance regulatory compliance with operational efficiency. This may involve using cloud providers with data centers in specific regions to ensure compliance while still leveraging the benefits of cloud services. Additionally, organizations must implement comprehensive data mapping practices to track where data is stored and processed, facilitating adherence to local regulations (Shahid *et al*al., 2022).

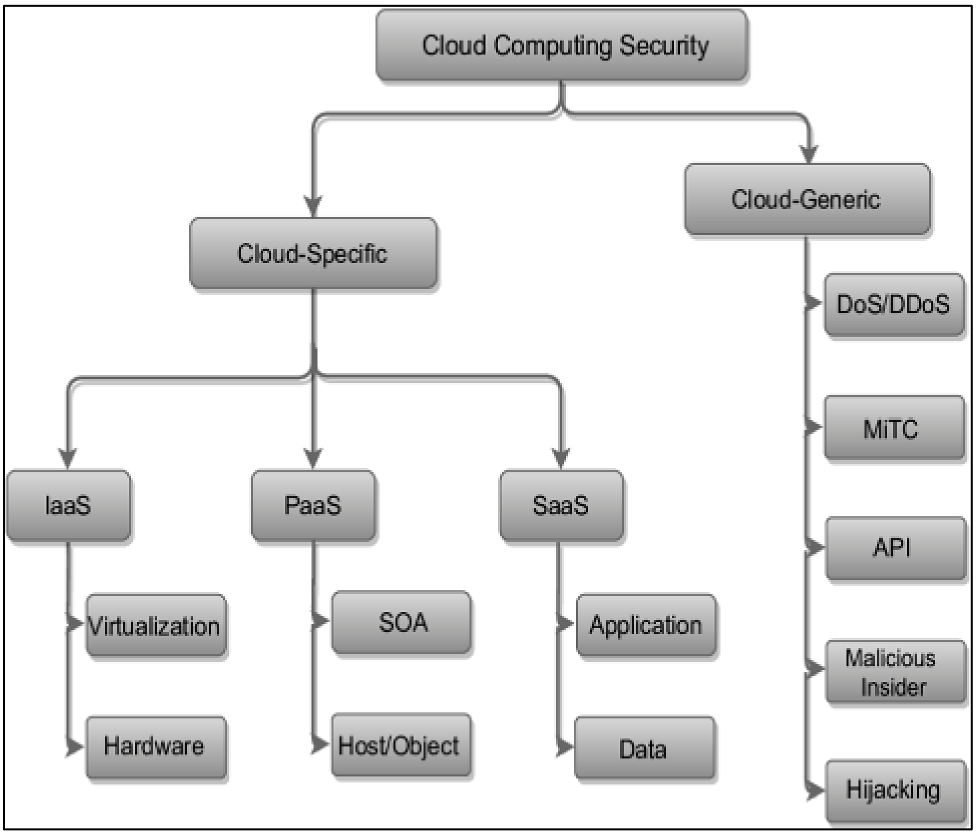

Figure 1 Taxonomy of Cloud Computing Security (Parast *et al*al., 2022)

Ensuring data integrity and availability is essential for maintaining compliance and building trust with stakeholders. Policies that guarantee data accuracy and consistency are critical, particularly when organizations rely on data for decision-making and operational processes. Regular audits and validation processes should be established to confirm the accuracy of data, thereby mitigating risks associated with data errors (Raji *et al*al., 2020). Backup and disaster recovery measures are equally vital for compliance assurance. Organizations must develop robust backup strategies that ensure data can be restored in the event of loss or corruption. Implementing disaster recovery plans that outline procedures for data restoration is crucial to maintaining business continuity while complying with legal obligations regarding data availability.

The components of data compliance in cloud computing are essential for organizations striving to navigate the complex landscape of regulatory obligations and security requirements. By addressing data privacy and protection, security and confidentiality, sovereignty and localization, as well as integrity and availability, organizations can create a comprehensive compliance framework that fosters responsible cloud adoption (Mitchell and Samlidis, 2021; Dawood *et al*al., 2023). As technology continues to evolve, these components will play a pivotal role in shaping the future of data compliance, enabling organizations to leverage cloud solutions while safeguarding sensitive information and adhering to legal mandates.

2.1. Framework for Implementing Data Compliance in Cloud Computing

As organizations increasingly adopt cloud computing solutions, ensuring data compliance has become a critical concern (Al-Marsy *et al*al., 2021). A robust framework for implementing data compliance is essential for safeguarding sensitive information while adhering to regulatory mandates as explain in figure 2 (Awaysheh *et al*al., 2021). This framework encompasses several key components, including risk assessment and mitigation, data governance and ownership, continuous monitoring and auditing, and incident management and response.

The first step in any compliance framework is conducting a comprehensive risk assessment tailored to the specific challenges of cloud environments. Organizations must identify potential compliance risks, including data breaches, non-compliance with regulations, and the misuse of sensitive information (Shukla *et al*al., 2022). This involves evaluating the types of data stored in the cloud, understanding the regulatory landscape, and assessing the security measures in place. Once risks are identified, organizations can develop strategies to mitigate them through a combination of policy and technology solutions. This may include establishing clear data handling policies that outline how data should be processed, stored, and accessed within the cloud environment. Additionally, implementing technological measures such as encryption, access controls, and multi-factor authentication can significantly reduce the likelihood of data breaches and unauthorized access (Aslam *et al*al., 2021).

Establishing clear data governance is vital for ensuring compliance within cloud environments. Organizations should define roles and responsibilities for data custodianship, delineating who is accountable for managing data at each stage of its lifecycle (Zhang *et al*al., 2022). This clarity helps to mitigate confusion regarding data ownership and facilitates compliance with regulations that require clear lines of responsibility. Guidelines for data ownership, access rights, and usage should be developed and communicated throughout the organization. This involves defining who has the authority to access specific datasets, under what circumstances, and for what purposes. By creating a structured governance model, organizations can better manage their data assets and ensure compliance with relevant regulations.

Continuous monitoring and auditing are essential components of an effective compliance framework. Real-time monitoring systems can help detect policy violations and security incidents as they occur, enabling organizations to respond promptly to potential threats (Kebande *et al*al., 2021). This proactive approach is crucial for identifying vulnerabilities before they can be exploited. Regular audits should also be conducted to ensure compliance with evolving regulations and internal policies. These audits serve as a critical tool for evaluating the effectiveness of the compliance framework and identifying areas for improvement. Organizations should establish a schedule for audits and ensure that they are conducted by qualified personnel who can provide an objective assessment of compliance efforts.

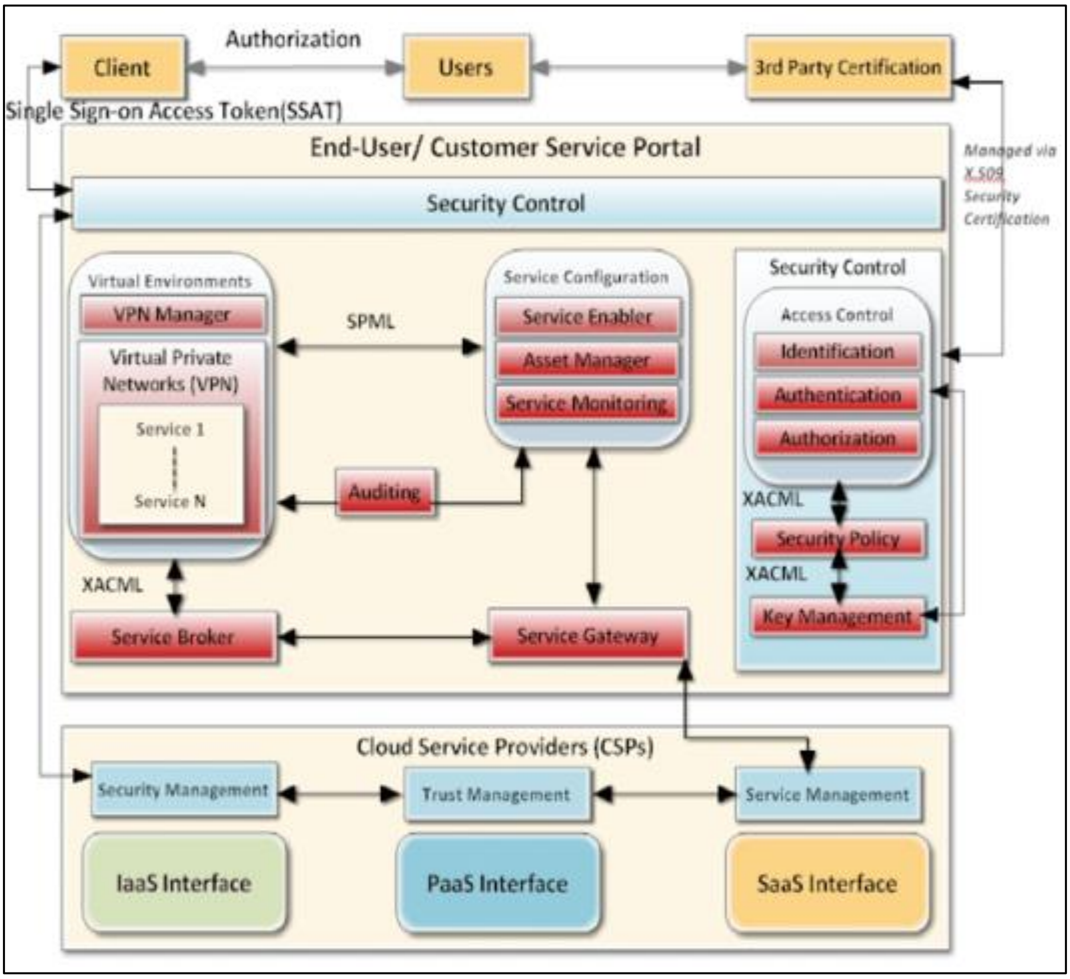

Figure 2 Structure for Safe Cloud Computing (Awaysheh *et al*al., 2021)

Despite best efforts, data breaches and compliance failures can still occur. An effective framework must include robust incident management and response procedures. Organizations should develop clear protocols for handling data breaches, including steps for containment, investigation, and notification of affected parties (Khan *et al*al., 2021). This is especially critical in light of regulations that require timely notification to regulators and individuals in the event of a data breach. Post-incident reviews are equally important for identifying the root causes of compliance issues and preventing future occurrences. These reviews should assess the effectiveness of the response to the incident and identify lessons learned. By fostering a culture of continuous improvement, organizations can enhance their compliance posture and better protect sensitive data in the cloud.

A comprehensive framework for implementing data compliance in cloud computing is essential for organizations navigating the complexities of regulatory requirements and data protection. By focusing on risk assessment and mitigation, data governance and ownership, continuous monitoring and auditing, and incident management and response, organizations can create a robust compliance strategy (Johannsen *et al*al., 2020; Abdulrasool and Turnbull, 2020). This approach not only safeguards sensitive information but also fosters trust with stakeholders and ensures that organizations remain compliant in an evolving regulatory landscape.

2.2. Technological Tools for Ensuring Compliance

In the rapidly evolving landscape of cloud computing and data management, organizations face increasing pressure to adhere to stringent compliance regulations (Levite and Kalwani, 2020). To me*et* these challenges, technological tools have emerged as essential assets for ensuring compliance across various domains, including data privacy, security, and regulatory adherence. This explores four significant technological tools for ensuring compliance: compliance automation tools, AI and machine learning applications, data loss prevention (DLP) and encryption solutions, and blockchain technology.

Compliance automation tools streamline various compliance tasks, significantly reducing manual effort and minimizing the risk of human error (Biswas and Dutta, 2020). These tools can automate processes such as data classification, which helps organizations identify and categorize sensitive information based on regulatory requirements. By employing automated data classification, organizations can ensure that sensitive data is handled appropriately and in accordance with legal obligations. Additionally, compliance automation tools facilitate encryption of sensitive data. They can automatically apply encryption protocols to data both at rest and in transit, ensuring that information is protected from unauthorized access. Furthermore, these tools often include audit logging functionalities, which automatically record actions taken on sensitive data. This logging capability is crucial for compliance audits, providing a clear trail of data access and modifications that can be reviewed by regulatory bodies.

Artificial intelligence (AI) and machine learning (ML) technologies are increasingly being integrated into compliance frameworks to enhance efficiency and effectiveness (Angehrn *et al*al., 2020; Shah, 2021). These technologies can analyze vast amounts of data to detect anomalies that may indicate compliance breaches or security incidents. By employing machine learning algorithms, organizations can establish baseline behaviors for data usage and identify deviations that warrant further investigation. Moreover, AI can enforce compliance policies at scale, automating responses to policy violations in real time. For example, if a user attempts to access sensitive data outside of their authorized parameters, AI-driven systems can automatically restrict access, notify compliance officers, and generate alerts. This proactive approach not only reduces the burden on compliance teams but also enhances the organization's overall security posture.

Data loss prevention (DLP) solutions play a vital role in protecting sensitive data throughout its lifecycle. DLP tools monitor and control data transfers, ensuring that sensitive information does not leave the organization without proper authorization. By implementing DLP technologies, organizations can enforce data handling policies and prevent unauthorized sharing or exposure of sensitive information (Rajendra, 2020). Encryption solutions are equally critical in safeguarding data, both in transit and at rest. These technologies encrypt sensitive information, making it unreadable to unauthorized users. During processing, encryption solutions can protect data in use, ensuring that even if a breach occurs, the data remains secure. By combining DLP and encryption technologies, organizations can create a comprehensive security framework that ensures compliance with data protection regulations.

Blockchain technology offers unique advantages in enhancing compliance efforts, particularly in terms of transparency and traceability (Dutta *et al*al., 2020). By leveraging a decentralized and immutable ledger, organizations can ensure that all transactions related to data access and modifications are recorded transparently. This transparency fosters trust among stakeholders, as all parties can independently verify compliance efforts. Additionally, blockchain's traceability features enable organizations to maintain comprehensive audit trails. Each transaction recorded on the blockchain is time-stamped and linked to a specific user, creating a verifiable history of data handling. This capability is invaluable for compliance audits, allowing organizations to demonstrate adherence to regulatory requirements with a high degree of accuracy and reliability.

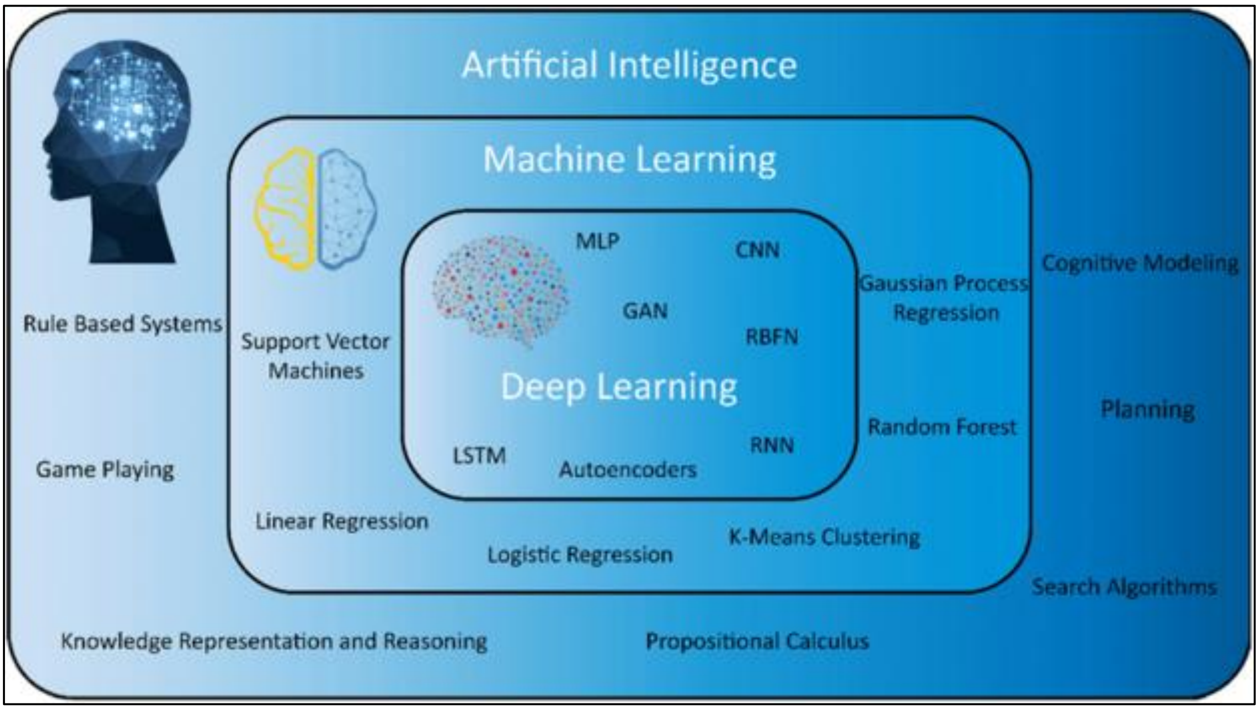

Figure 3 Domains of popular algorithms, AI, ML, and DL (Baduge *et al*al., 2022)

Technological tools play a pivotal role in ensuring compliance within cloud computing and data management environments. Compliance automation tools streamline essential tasks, while AI and machine learning enhance detection and enforcement capabilities. DLP and encryption solutions provide robust protection for sensitive data, and blockchain technology introduces a new level of transparency and traceability to compliance efforts (Sedlmeir *et al*al., 2022). As organizations continue to navigate complex regulatory landscapes, embracing these technological tools will be crucial for maintaining compliance and safeguarding sensitive information.

2.3. Best Practices for Ensuring Data Compliance

Ensuring data compliance is a critical aspect of managing information in today's digital landscape, particularly with the increasing reliance on cloud computing and the ever-evolving regulatory environment (Miryala and Gupta, 2022). Organizations must implement best practices to effectively navigate compliance challenges and protect sensitive data. This highlights three key best practices: employee training and awareness, vendor and third-party compliance management, and regular policy updates and compliance reviews.

One of the most significant aspects of ensuring data compliance is fostering a culture of awareness and accountability among employees. Training programs should be established to educate staff on data compliance protocols, relevant laws, and security practices. By empowering employees with knowledge about compliance requirements, organizations can reduce the risk of unintentional violations and enhance their overall security posture (Dhillon *et al*al., 2020). Training should encompass various topics, including data handling procedures, the significance of data privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and the importance of reporting potential compliance issues. Regular training sessions and awareness campaigns can help reinforce these concepts, ensuring that employees remain vigilant and informed about their roles in maintaining compliance. Furthermore, organizations should create a feedback loop that encourages employees to share insights and concerns regarding data compliance, which can lead to improved policies and practices.

In an increasingly interconnected digital ecosystem, organizations often rely on third-party vendors and service providers to manage and store sensitive data (Das, 2020). This reliance necessitates a robust vendor compliance management program to ensure that third parties adhere to the same compliance standards as the organization itself. To manage vendor compliance effectively, organizations should conduct thorough due diligence during the vendor selection process. This includes evaluating vendors' security practices, compliance certifications, and their ability to me*et al*regulatory requirements. Organizations should also establish contractual obligations that explicitly define compliance expectations, data handling practices, and the right to conduct audits. Moreover, ongoing monitoring of vendor compliance is crucial. Regular assessments and audits can help identify potential vulnerabilities and ensure that third parties maintain compliance standards. Organizations should also develop contingency plans to address any compliance breaches or failures on the part of vendors, minimizing potential risks to sensitive data.

The landscape of data compliance is continually changing, driven by advancements in technology, evolving regulations, and shifting organizational needs as explain in figure 4 (Bognár and Benedek, 2021). As such, organizations must implement a structured process for regularly reviewing and updating their compliance policies. This proactive approach ensures that policies remain relevant and effective in addressing current compliance challenges. Organizations should establish a schedule for policy reviews, aligning them with industry best practices and regulatory changes. During these reviews, organizations should assess the effectiveness of existing policies, identify areas for improvement, and incorporate feedback from employees and stakeholders (Camilleri, 2021). It is essential to remain informed about developments in data protection laws and emerging compliance trends, as these factors can influence organizational policies. Additionally, organizations should implement a system for tracking compliance metrics and performance indicators. This data can provide valuable insights into the effectiveness of compliance efforts and help identify potential gaps in policies. By continually evaluating and adapting compliance policies, organizations can maintain a robust compliance framework that meets their evolving needs.

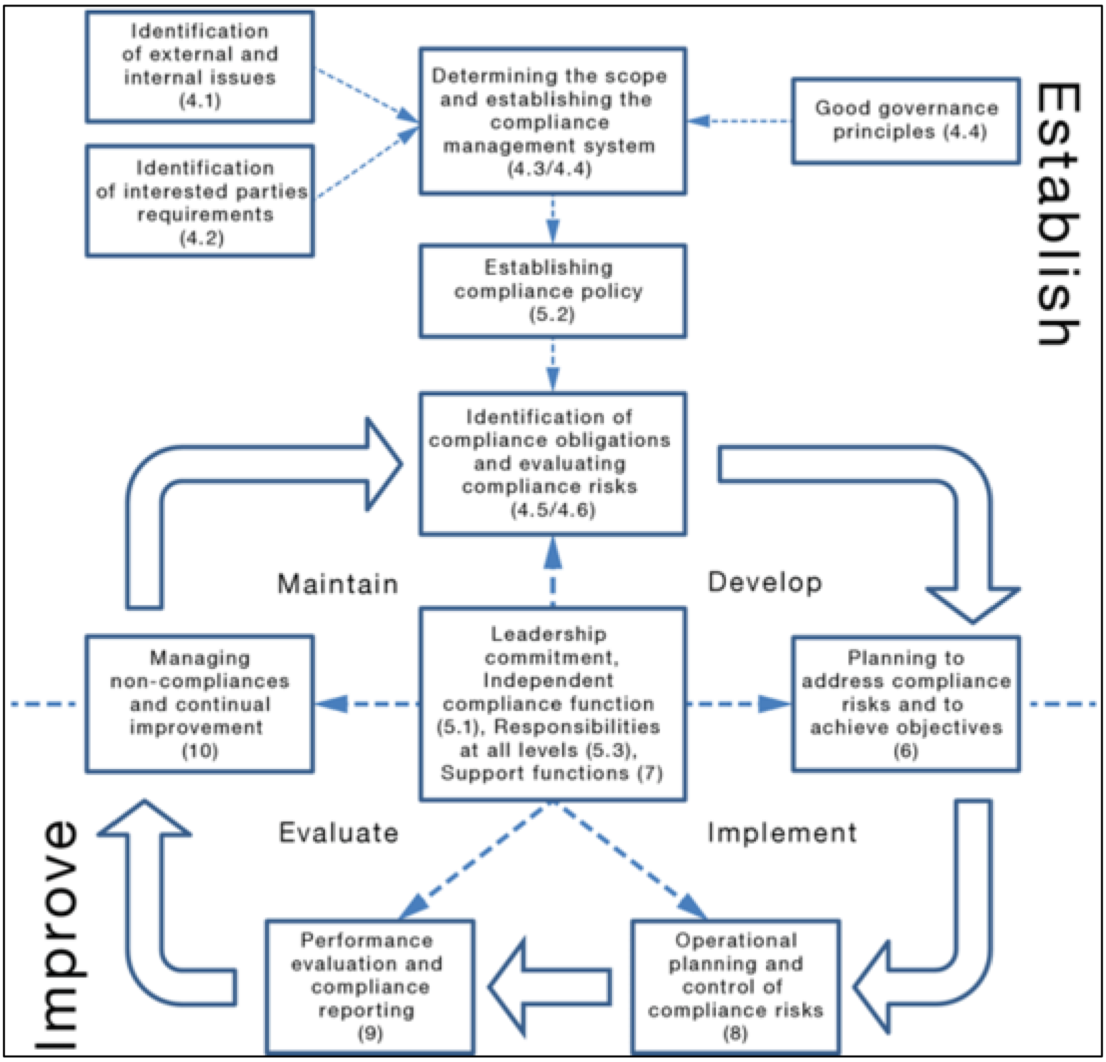
Identification of external and internal issues (4.1)
Identification of interested parties requirements (4.2)
Determining the scope and establishing the compliance management system (4.3/4.4)
Good governance principles (4.4)
Establish
Establishing compliance policy (5.2)
Identification of compliance obligations and evaluating compliance risks (4.5/4.6)
Maintain
Develop
Managing non-compliances and continual improvement (10)
Leadership commitment, Independent compliance function (5.1), Responsibilities at all levels (5.3), Support functions (7)
Planning to address compliance risks and to achieve objectives (6)
Evaluate
Implement
Improve
Performance evaluation and compliance reporting (9)
Operational planning and control of compliance risks (8)

Figure 4 Flowchart for a compliance management system (Bognár and Benedek, 2021)

Best practices for ensuring data compliance are essential for organizations navigating the complexities of the digital landscape. By prioritizing employee training and awareness, implementing effective vendor and third-party compliance management, and conducting regular policy updates and compliance reviews, organizations can establish a strong compliance culture (Weston and Hoopes, 2021; Salih *et al*al., 2021). These practices not only mitigate the risk of compliance violations but also foster trust among stakeholders, ensuring the protection of sensitive data in an increasingly interconnected world.

2.4. Challenges in Data Compliance for Cloud Environments

The rapid growth of cloud computing has revolutionized data storage, processing, and management, enabling organizations to operate with unprecedented flexibility and scale (Valleru and Alapati, 2022). However, maintaining data compliance within cloud environments presents unique challenges due to the complexity of multi-cloud and hybrid setups, an evolving regulatory landscape, and inherent data privacy and security risks. Each of these challenges requires a strategic approach to ensure compliance while optimizing cloud utility.

As organizations increasingly adopt multi-cloud and hybrid cloud architectures, compliance challenges become more pronounced (Sathupadi, 2022). Multi-cloud environments involve the use of multiple cloud service providers (CSPs), often with varying service models and infrastructure configurations. Hybrid cloud setups combine public and private clouds, which allows for enhanced data control but introduces added complexity in maintaining a unified compliance framework. In multi-cloud and hybrid setups, organizations face difficulties in enforcing consistent compliance policies across diverse platforms. Each CSP may offer different tools for data protection, security, and privacy, complicating policy standardization. For example, managing access controls, encryption standards, and data classification in a consistent manner becomes challenging when working across different cloud environments with unique capabilities and configurations. Furthermore, compliance requirements may vary depending on the jurisdiction in which each CSP operates, which can lead to inconsistencies in data handling practices and potential regulatory breaches (Peihani, 2022). To address these issues, organizations must adopt a flexible, platform-agnostic compliance strategy that includes policies applicable across various cloud environments. Additionally, implementing cloud-agnostic security tools, such as encryption and identity management solutions, can help maintain compliance in multi-cloud and hybrid setups by providing consistent data protection and security measures.

One of the most significant challenges for data compliance in cloud environments is navigating the evolving landscape of data protection regulations across different regions. Data protection laws, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose stringent requirements for data handling, processing, and storage (Blanke, 2020' Niebel, 2021). While these regulations are essential for protecting individual privacy, they present complexities for organizations operating in global cloud environments. Each regulatory framework has unique requirements, which can create conflicts or inconsistencies in compliance practices. For example, data localization requirements, where certain types of data must remain within specific geographic boundaries, pose challenges for organizations that store data across multiple CSPs located in different regions. Organizations must frequently monitor regulatory changes to ensure that their cloud environments remain compliant, a task that requires substantial resources and expertise. Furthermore, the lack of standardized regulations across countries complicates cross-border data transfers, leading to potential compliance issues and legal risks. To manage this challenge, organizations should invest in regulatory intelligence systems and stay informed of changes in data protection laws. Collaborating with legal and compliance experts can also help organizations interpr*et al*and implement regulatory requirements effectively. Additionally, cloud providers are increasingly offering compliance certifications and regional data centers, which can assist organizations in meeting specific jurisdictional requirements (Saini *et al*al., 2022).

Data privacy and security remain top concerns for organizations in cloud environments, especially when balancing compliance with accessibility and usability. Cloud environments often store and process large volumes of sensitive data, making them a targ*et al*for cyberattacks and data breaches (Riaz *et al*al., 2020). In a compliance context, any data breach or unauthorized access can lead to significant penalties, reputational damage, and legal repercussions, particularly under regulations like GDPR and CCPA. Maintaining data privacy and security in the cloud involves implementing robust measures, such as encryption, access controls, and data masking, while ensuring that these safeguards do not hinder operational efficiency. However, achieving this balance is difficult, as overly restrictive security measures can limit data accessibility, reducing the cloud's usability and negating its advantages. In addition, cloud environments are susceptible to shared-responsibility complexities, where the cloud provider and the client both share security obligations, which may lead to misunderstandings or gaps in compliance efforts. Organizations can address these privacy and security challenges by developing a clear understanding of shared responsibilities and ensuring that both they and their cloud providers me*et al*compliance obligations. Regular audits, security assessments, and incident response plans are essential to detect and mitigate security risks. Additionally, employing privacy-enhancing technologies (PETs), such as homomorphic encryption or secure multiparty computation, can help balance data accessibility with privacy protection (Soykan *et al*al., 2022).

Data compliance in cloud environments presents significant challenges due to the complexity of multi-cloud and hybrid architectures, the constantly evolving regulatory landscape, and inherent data privacy and security risks. To navigate these challenges effectively, organizations need to adopt flexible, proactive strategies and leverage advanced technological tools to ensure compliance without compromising cloud functionality. By understanding these key compliance challenges, organizations can better safeguard their data, maintain regulatory alignment, and realize the benefits of cloud computing in a secure and compliant manner (Ali and Osmanaj, 2020)

2.5. Future Directions for Data Compliance in Cloud Computing

As cloud computing continues to transform industries, data compliance frameworks must evolve to me*et al*increasingly complex regulatory and security challenges (Mohlameane and Ruxwana, 2020). Future directions in data compliance will likely emphasize advanced technologies and collaborative regulatory approaches, including the integration of AI for dynamic compliance management, the development of global compliance standards, and advancements in privacy-preserving technologies. These innovations promise to enhance data security, streamline compliance, and foster trust in cloud environments.

Artificial intelligence (AI) holds significant potential for managing data compliance dynamically within cloud environments. Traditional compliance methods, often manual and reactive, struggle to keep pace with the rapid changes in cloud infrastructure, applications, and regulatory requirements. AI-driven compliance management can adapt to evolving data protection needs in real-time, offering automated detection, monitoring, and response to compliance risks (Polamarasetti, 2022). Machine learning algorithms, for instance, can continuously scan cloud environments to detect non-compliant activities, flagging and remediating issues before they escalate into regulatory violations. Moreover, AI's predictive capabilities allow organizations to anticipate compliance risks and implement proactive measures, a key advantage in multi-cloud and hybrid environments where data handling practices differ. AI-based solutions can also streamline policy enforcement by automatically applying relevant policies based on the data's location, usage, and sensitivity. As regulations become increasingly complex and granular, dynamic AI-driven compliance systems can reduce human error, enhance accuracy, and minimize the costs of regulatory adherence. However, adopting AI for compliance will require investment in technology and skilled personnel to effectively manage these tools and ensure alignment with regulatory standards (Lescrauwa*et alet al*al., 2022).

As cloud computing transcends national borders, a fragmented regulatory landscape poses challenges for organizations operating in multiple jurisdictions (Arner *et al*al., 2022). Moving towards a harmonized regulatory approach to data compliance, especially at the global level, could significantly reduce compliance burdens and risks associated with cross-border data transfers. Currently, data compliance standards differ across regions, with frameworks such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the USA, and emerging regulations in other parts of the world. A unified, globally recognized compliance framework would simplify regulatory requirements for organizations and facilitate safer data flows across borders. International regulatory bodies and collaborative initiatives, such as the International Organization for Standardization (ISO), are actively working towards setting global standards that promote data protection while supporting international business needs. Harmonized compliance standards can also aid in establishing a clear framework for cloud providers, helping them to develop data processing infrastructures that me*et al*global expectations (Katari and Ankam, 2022). For such efforts to succeed, cross-national collaboration is essential, including regulatory partnerships that ensure compliance frameworks are both adaptable and robust enough to address unique regional needs.

Emerging privacy-preserving technologies (PPTs) are crucial for enhancing data compliance in cloud environments. Homomorphic encryption, secure multi-party computation, and federated learning are among the most promising tools that allow data to be processed without compromising user privacy. Homomorphic encryption enables computations on encrypted data, so sensitive information can be analyzed without decrypting it, thereby minimizing exposure risks in the cloud (Vamsi and Reddy, 2022). This is especially relevant for industries handling sensitive data, such as healthcare and finance, where privacy and compliance requirements are stringent. Secure multi-party computation (SMPC) allows multiple parties to jointly compute a function over their inputs without disclosing the actual data. This technology is particularly useful for collaborative environments where compliance requirements demand high levels of data confidentiality. Federated learning is another promising approach that enables machine learning models to be trained on decentralized data, reducing the need for data transfers and enhancing compliance with data localization laws (Yin *et al*al., 2020). These technologies collectively provide cloud service providers and organizations with robust tools for ensuring privacy, supporting data sovereignty requirements, and managing data across complex, distributed cloud infrastructures.

Future directions in data compliance for cloud computing are poised to integrate AI-driven compliance management, foster global regulatory collaboration, and leverage cutting-edge privacy-preserving technologies. AI offers the potential for adaptive, real-time compliance, while global standards could streamline regulatory requirements and simplify cross-border data handling. Privacy-preserving technologies further support compliance efforts by minimizing data exposure risks. These advancements collectively promise to create a more secure and compliant cloud environment, providing organizations with the tools and frameworks needed to navigate an increasingly complex regulatory landscape while capitalizing on the benefits of cloud computing.

3. Conclusion

Data compliance in cloud computing demands a structured, multi-faceted approach to effectively safeguard data and me*et al*regulatory requirements. Key components of a robust data compliance model include data privacy and protection, data security and confidentiality, data sovereignty, and data integrity and availability. Together, these elements form a comprehensive framework that enables organizations to maintain compliance across complex cloud environments. To implement this model, organizations should conduct regular risk assessments, establish clear data governance structures, engage in continuous monitoring, and develop a responsive incident management protocol. By addressing each of these components, organizations can create a solid foundation for protecting sensitive data and ensuring regulatory adherence.

Adopting a proactive approach to compliance is essential in the fast-evolving landscape of cloud computing. Reactive measures often fall short in addressing the dynamic risks associated with cloud environments and shifting regulatory demands. By implementing ongoing training, regularly updating policies, and utilizing real-time monitoring tools, organizations can anticipate and mitigate compliance challenges before they lead to potential violations. This proactive stance not only strengthens data protection but also enhances trust with stakeholders, customers, and regulatory authorities.

As cloud technologies and regulatory standards continue to evolve, organizations must remain flexible and adapt their compliance models accordingly. Emerging technologies such as AI, privacy-preserving tools, and automated compliance solutions are s*et al*to play an increasingly important role in supporting compliance efforts. In this context, a model that embraces adaptability and innovation will allow organizations to respond effectively to new challenges and maintain compliance in a future marked by rapid technological advancement and heightened data governance expectations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdulrasool, F.E. and Turnbull, S.J., 2020. Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. *International Journal of Electronic Banking*, *2*(3), pp.237-265.

[2] Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z., 2021. Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), p.16.

[3] Ahsan, A. and Shabbir, A., 2021. Blockchain and Big Data: Exploring Convergence for Privacy, Security and Accountability. *Sage Science Review of Educational Technology*, *4*(2), pp.53-68.

[4] Ali, O. and Osmanaj, V., 2020. The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law & Security Review*, *36*, p.105396.

[5] Al-Marsy, A., Chaudhary, P. and Rodger, J.A., 2021. A model for examining challenges and opportunities in use of cloud computing for health information systems. *Applied System Innovation*, *4*(1), p.15.

[6] Angehrn, Z., Haldna, L., Zandvliet, A.S., Gil Berglund, E., Zeeuw, J., Amzal, B., Cheung, S.A., Polasek, T.M., Pfister, M., Kerbusch, T. and Heckman, N.M., 2020. Artificial intelligence and machine learning applied at the point of care. *Frontiers in pharmacology*, *11*, p.759.

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

[8] Aslam, S., Mumtaz, M., Ali, K. and Ilyas, M., 2021. Strengthening E-commerce Security: Utilizing Multi-Factor Authentication and Cyber Forensics for Threat Prevention.

[9] Awaysheh, F.M., Aladwan, M.N., Alazab, M., Alawadi, S., Cabaleiro, J.C. and Pena, T.F., 2021. Security by design for big data frameworks over cloud computing. *IEEE Transactions on Engineering Management*, *69*(6), pp.3676-3693.

[10] Baduge, S.K., Thilakarathna, S., Perera, J.S., Arashpour, M., Sharafi, P., Teodosio, B., Shringi, A. and Mendis, P., 2022. Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications. *Automation in Construction*, *141*, p.104440.

[11] Biswas, A. and Dutta, P.K., 2020, January. Novel approach of automation to risk management: The reduction in human errors. In *International Conference on Mobile Computing and Sustainable Informatics* (pp. 683-696). Cham: Springer International Publishing.

[12] Blanke, J.M., 2020. Protection for 'Inferences drawn': A comparison between the general data protection regulation and the california consumer privacy act. *Global Privacy Law Review*, *1*(2).

[13] Bognár, F. and Benedek, P., 2021. A Novel Risk Assessment Methodology—A Case Study of the PRISM Methodology in a Compliance Management Sensitive Sector. *Acta Polytechnica Hungarica*, *18*(7), pp.89-108.

[14] Camilleri, M.A., 2021. Evaluating service quality and performance of higher education institutions: a systematic review and a post-COVID-19 outlook. *International Journal of Quality and Service Sciences*, *13*(2), pp.268-281.

[15] Carlson, G., McKinney, J., Slezak, E. and Wilmot, E.S., 2020. General Data Protection Regulation and California Consumer Privacy Act: Background. *Currents: J. Int'l Econ. L.*, *24*, p.62.

[16] Das, A., 2020. Trust in "trust-free" digital networks: How inter-firm algorithmic relationships embed the cardinal principles of value co-creation. *AIS Transactions on Human-Computer Interaction*, *12*(4), pp.228-252.

[17] Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M. and Rehman, S.U., 2023. Cyberattacks and security of cloud computing: a complete guideline. *Symmetry*, *15*(11), p.1981.

[18] Dhillon, G., Abdul Talib, Y.Y. and Picoto, W.N., 2020. The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), p.5.

[19] Dutta, P., Choi, T.M., Somani, S. and Butala, R., 2020. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, *142*, p.102067.

[20] Hartzog, W. and Richards, N., 2020. Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, p.1687.

[21] Huising, R. and Silbey, S.S., 2021. Accountability infrastructures: Pragmatic compliance inside organizations. *Regulation & Governance*, *15*, pp.S40-S62.

[22] Johannsen, A., Kant, D. and Creutzburg, R., 2020. Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. *Electronic Imaging*, *32*, pp.1-11.

[23] Katari, A. and Ankam, M., 2022. Data Governance in Multi-Cloud Environments for Financial Services: Challenges and Solutions. *Educational Research (IJMCER)*, *4*(1), pp.339-353.

[24] Kebande, V.R., Karie, N.M. and Ikuesan, R.A., 2021. Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, *13*(1), pp.5-17.

[25] Khan, F., Kim, J.H., Mathiassen, L. and Moore, R., 2021. Data breach management: An integrated risk model. *Information & Management*, *58*(1), p.103392.

[26] Lancieri, F., 2022. Narrowing data protection's enforcement gap. *Me. L. Rev.*, *74*, p.15.

[27] Lescrauwaet, L., Wagner, H., Yoon, C. and Shukla, S., 2022. Adaptive legal frameworks and economic dynamics in emerging tech-nologies: Navigating the intersection for responsible innovation. *Law and Economics*, *16*(3), pp.202-220.

[28] Levite, A.E. and Kalwani, G., 2020. *Cloud governance challenges: A survey of policy and regulatory issues*. Washington, DC: Carnegie Endowment for International Peace.

[29] Lukings, M. and Habibi Lashkari, A., 2022. Data sovereignty. In *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective* (pp. 1-38). Cham: Springer International Publishing.

[30] Miryala, N.K. and Gupta, D., 2022. Data Security Challenges and Industry Trends. *IJARCCE International Journal of Advanced Research in Computer and Communication Engineering*, *11*(11), pp.300-309.

[31] Mitchell, A.D. and Samlidis, T., 2021. Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology*, *29*(4), pp.364-394.

[32] Mohlameane, M. and Ruxwana, N., 2020. Exploring the impact of cloud computing on existing South African regulatory frameworks. *South African Journal of Information Management*, *22*(1), pp.1-9.

[33] Muhammad, T., Munir, M.T., Munir, M.Z. and Zafar, M.W., 2022. Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), pp.99-135.

[34] Niebel, C., 2021. The impact of the general data protection regulation on innovation and the global political economy. *Computer Law & Security Review*, *40*, p.105523.

[35] Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S., 2022. Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, p.102580.

[36] Patil, P., Sangeetha, M. and Bhaskar, V., 2021. Blockchain for IoT access control, security and privacy: a review. *Wireless Personal Communications*, *117*(3), pp.1815-1834.

[37] Peihani, M., 2022. Regulation of cyber risk in the banking system: a Canadian case study. *Journal of Financial Regulation*, *8*(2), pp.139-161.

[38] Polamarasetti, A., 2022. AI-Driven Data Science for Enhanced Cloud Security and Compliance. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), pp.320-351.

[39] Rajendra, G.T.R.N., 2020. GUARDING CUSTOMER SECRETS: ESSENTIAL DATA PRIVACY AND SECURITY STRATEGIES FOR CRM AND ERP SYSTEMS. *INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)*, *11*(2), pp.611-638.

[40] Raji, I.D., Smart, A., White, R.N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D. and Barnes, P., 2020, January. Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 33-44).

[41] Riaz, S., Khan, A.H., Haroon, M., Latif, S. and Bhatti, S., 2020, August. Big data security and privacy: Current challenges and future research perspective in cloud environment. In *2020 International Conference on Information Management and Technology (ICIMTech)* (pp. 977-982). IEEE.

[42] 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.

[43] Salih, S., Hamdan, M., Abdelmaboud, A., Abdelaziz, A., Abdelsalam, S., Althobaiti, M.M., Cheikhrouhou, O., Hamam, H. and Alotaibi, F., 2021. Prioritising organisational factors impacting cloud ERP adoption and the critical issues related to security, usability, and vendors: A systematic literature review. *Sensors*, *21*(24), p.8391.

[44] Sathupadi, K., 2022. Ai-driven qos optimization in multi-cloud environments: Investigating the use of ai techniques to optimize qos parameters dynamically across multiple cloud providers. *Applied Research in Artificial Intelligence and Cloud Computing*, *5*(1), pp.213-226.

[45] Sedlmeir, J., Lautenschlager, J., Fridgen, G. and Urbach, N., 2022. The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), pp.1779-1794.

[46] Segijn, C.M., Strycharz, J., Riegelman, A. and Hennesy, C., 2021. A literature review of personalization transparency and control: Introducing the Transparency-Awareness-Control Framework. *Media and Communication*, *9*(4), pp.120-133.

[47] Shah, V., 2021. Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), pp.42-66.

[48] Shahid, J., Ahmad, R., Kiani, A.K., Ahmad, T., Saeed, S. and Almuhaideb, A.M., 2022. Data protection and privacy of the intern*et al*of healthcare things (IoHTs). *Applied Sciences*, *12*(4), p.1927.

[49] Shepherd, M., Turner, J.A., Small, B. and Wheeler, D., 2020. Priorities for science to overcome hurdles thwarting the full promise of the 'digital agriculture'revolution. *Journal of the Science of Food and Agriculture*, *100*(14), pp.5083-5092.

[50] Shneiderman, B., 2020. Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *10*(4), pp.1-31.

[51] Shukla, S., George, J.P., Tiwari, K. and Kureethara, J.V., 2022. Data security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.

[52] Soykan, E.U., Karacay, L., Karakoc, F. and Tomur, E., 2022. A survey and guideline on privacy enhancing technologies for collaborative machine learning. *IEEE Access*, *10*, pp.97495-97519.

[53] Srivastava, S.K. and Bag, S., 2023. Recent developments on flexible manufacturing in the digital era: A review and future research directions. *Global Journal of Flexible Systems Management*, *24*(4), pp.483-516.

[54] Sung, C.S. and Park, J.Y., 2021. Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, *34*(5), pp.1481-1505.

[55] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.

[56] Valleru, V. and Alapati, N.K., 2022. Serverless Architectures and Automation: Redefining Cloud Data Management. *MZ Computing Journal*, *3*(2).

[57] Vamsi, D. and Reddy, P., 2022. Electronic health record security in cloud: Medical data protection using homomorphic encryption schemes. In *Research Anthology on Securing Medical Systems and Records* (pp. 853-877). IGI Global.

[58] Weston, L. and Hoopes, J., 2021. Best practices in compliance training. *Journal of Financial Compliance*, *4*(3), pp.282-291.

[59] Yanamala, A.K.Y. and Suryadevara, S., 2023. Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), pp.294-319.

[60] Yin, F., Lin, Z., Kong, Q., Xu, Y., Li, D., Theodoridis, S. and Cui, S.R., 2020. FedLoc: Federated learning framework for data-driven cooperative localization and location data processing. *IEEE Open Journal of Signal Processing*, *1*, pp.187-215.

[61] Zhang, J., Symons, J., Agapow, P., Teo, J.T., Paxton, C.A., Abdi, J., Mattie, H., Davie, C., Torres, A.Z., Folarin, A. and Sood, H., 2022. Best practices in the real-world data life cycle. *PLOS digital health*, *1*(1), p.e0000003.