Data Privacy and Compliance in the Cloud (GDPR, HIPAA, CCPA)

Kishan Raj Bellala[1]

[1]Affiliation: Independent Researcher

[1]ORCID ID: https://orcid.org/0009-0007-2327-0993

[1]Location: Austin, Texas, U.S.A.

Publication Date: 2025/07/26

Abstract: Organizations that move their operations to cloud-based infrastructure face rising concerns about data privacy and regulatory compliance because of their need for enhanced agility and scalability and cost efficiency. This research investigates the intricate process of protecting data privacy within cloud environments through an examination of GDPR and HIPAA and CCPA regulatory requirements. The three regulations establish separate requirements which organizations must follow when handling personal data throughout their entire lifecycle from collection to storage and processing and data transfer. The paper examines how cloud environments create difficulties for organizations to meet regulatory requirements through their impact on data residency and shared responsibility models and visibility into data flows. The paper presents organizations with the best practices and strategies to maintain privacy standards when using cloud services by implementing robust vendor management and data encryption and compliance monitoring. The paper provides forward-thinking perspectives to demonstrate why organizations must embed privacy and compliance fundamentals into their cloud strategies to establish trust and minimize risks and maintain regulatory compliance in the digital age.

Keywords: *Data Privacy, Regulatory Compliance, GDPR, HIPAA, CCPA, Cloud Infrastructure, Data Residency, Shared Responsibility Model, Data Lifecycle, Personal Data Protection, Data Storage, Data Processing, Data Transfer, Vendor Management, Encryption, Compliance Monitoring, Privacy Strategies, Digital Trust, Risk Mitigation.*

How to Cite: Kishan Raj Bellala (2025), Data Privacy and Compliance in the Cloud (GDPR, HIPAA, CCPA). *International Journal of Innovative Science and Research Technology*, 10(7), 2091-2097. https://doi.org/10.38124/ijisrt/25jul1264

I. INTRODUCTION

Modern IT strategies now depend heavily on cloud computing because they provide organizations with scalable infrastructure and flexible operations and cost-effective solutions (Samant, 2024). The growing movement of businesses to cloud-based operations and data storage systems has caused a substantial transformation in data management practices. The transition to cloud-based operations creates major challenges because data privacy and regulatory compliance stand as the most critical issues (Samant, 2024).

Data in the cloud moves between multiple geographical areas while being stored on infrastructure which the data owner cannot directly control (Fayayola, 2024). The situation creates specific security risks which demand answers about who should protect confidential information. The distributed and virtualized cloud environment creates challenges for organizations to maintain visibility and enforce consistent security measures while ensuring control across all touchpoints. The expanding number of worldwide data protection regulations makes these challenges even more difficult to overcome (Fayayola, 2024).

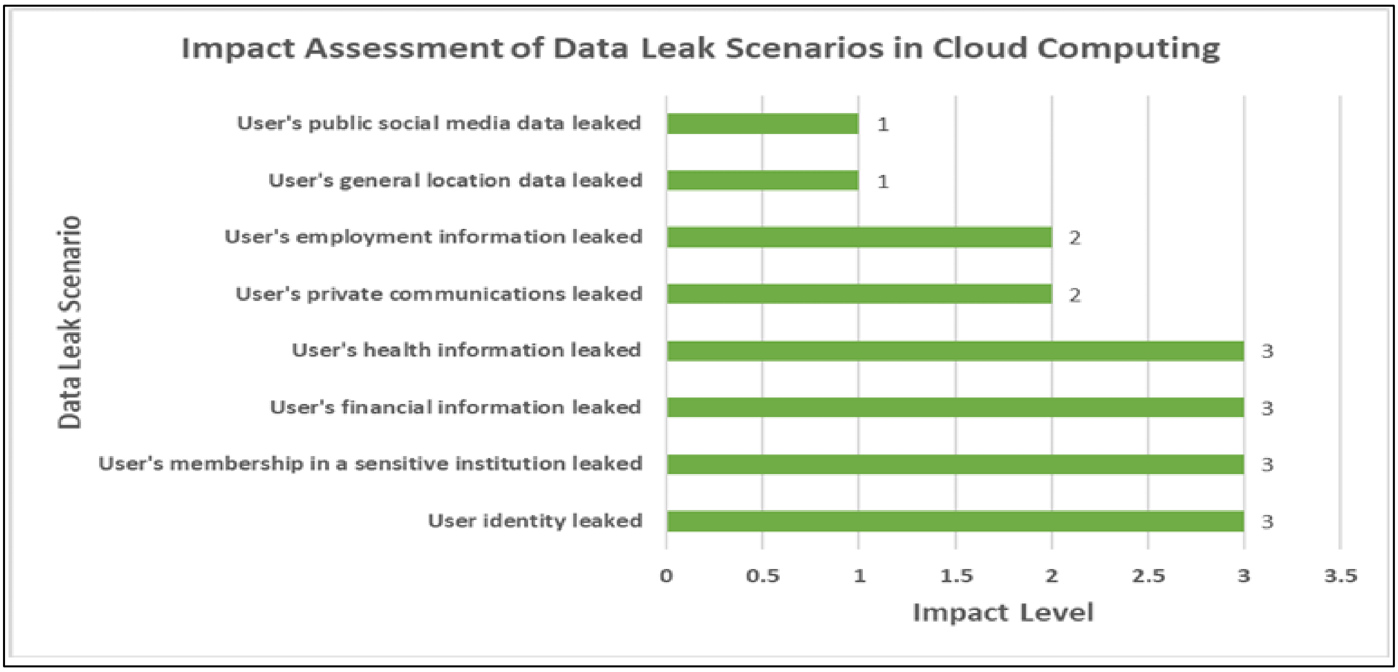


Fig 1 Impact of the Data Leak Scenarios (Samant, 2024).

From Figure 1 we can see the impact of data leaks in various scenarios for cloud computing. The General Data Protection Regulation (GDPR) of the European Union together with the Health Insurance Portability and Accountability Act (HIPAA) of the United States and the California Consumer Privacy Act (CCPA) represent the most influential regulatory standards (Maddali, 2024).

Organizations must follow strict data handling requirements under these regulatory frameworks starting from data collection all the way to storage and processing and transfer operations. Organizations that fail to comply with these laws must face substantial financial penalties and suffer damage to their reputation and legal repercussions (Fayayola, 2024).

II. UNDERSTANDING CLOUD DATA PRIVACY

Organizations moving to cloud computing for scalability and cost benefits must address privacy and compliance challenges. Cloud environments create complexities in protecting sensitive information beyond traditional IT infrastructure (Maddali, 2024).

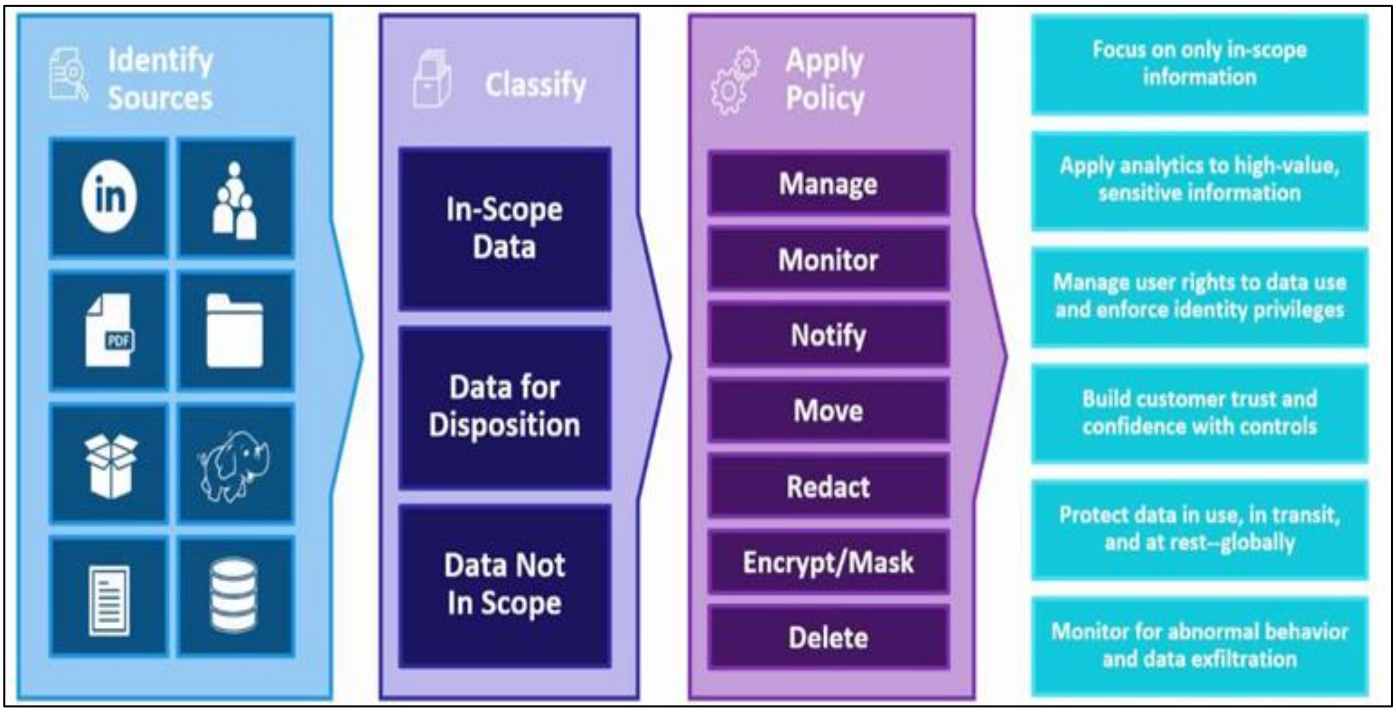

Identify Sources
Classify
In-Scope Data
Data for Disposition
Data Not In Scope
Apply Policy
Manage
Monitor
Notify
Move
Redact
Encrypt/Mask
Delete
Focus on only in-scope information
Apply analytics to high-value, sensitive information
Manage user rights to data use and enforce identity privileges
Build customer trust and confidence with controls
Protect data in use, in transit, and at rest–globally
Monitor for abnormal behavior and data exfiltration

Fig 2 Data Privacy Frame work (Maddali, 2024).

The following section describes the main privacy issues in cloud computing.

➢ *Data Storage Across Jurisdictions:*

Cloud providers operate data centers across multiple countries. This distributed model provides redundancy but creates legal issues as data falls under storage location laws (Kshetri, 2013). The GDPR applies to EU centers while U.S. laws govern American data storage. Multiple jurisdictions create challenges in meeting regulatory requirements. Organizations must handle global data exchanges through Binding Corporate Rules (BCRs) or Standard Contractual Clauses (SCCs). Improper data location management risks regulatory violations and loss of consumer trust (Kshetri, 2013).

➢ *Shared Responsibility Model (Cloud Provider vs. Customer):*

This model divides responsibilities based on service type (IaaS, PaaS, or SaaS).

- Cloud providers protect infrastructure through physical servers, networking and hypervisors (Pearson, 2010).
- Customers must secure data, user access, configurations and applications (Pearson, 2010).

Unclear responsibility definitions create protection gaps. Customers often mistakenly assume default data encryption, leading to asset exposure risks (Pearson, 2010).

➢ *Data Breaches and Unauthorized Access:*

Cloud environments risk data breaches through system vulnerabilities including misconfigurations and compromised credentials (Thoom, 2025). Centralized architecture attracts criminals who can access multiple datasets through single breaches. Unauthorized access occurs through vendor employees and staff. GDPR, HIPAA and CCPA enforce breach of notification requirements and penalties (Yusuff, 2023).

➢ *Lack of Visibility and Control Over Data:*

Organizations maintain complete control over data through traditional on-premises setups. Cloud reduces visibility as data passes through multiple systems managed by external providers, making tracking difficult (Thoom, 2025). This lack of transparency creates difficulties for compliance audits and policy enforcement. GDPR requires organizations to delete personal data when individuals request it. Limited control in cloud environments makes meeting regulatory requirements and detecting suspicious activities more difficult, increasing risk (Yusuff, 2023).

III. OVERVIEW OF KEY DATA PRIVACY FRAMEWORKS

➢ *General Data Protection Regulation (GDPR):*

The General Data Protection Regulation (GDPR) is introduced in May 2018 to enhance data protection for EU citizens. GDPR applies to all organizations handling EU residents' personal data, including those offering goods or services in the EU. Organizations must ensure compliance to avoid penalties of up to 4% of annual global revenue or €20 million (Fakeyede, 2023).

- *Fundamental Rules:*

✓ **Lawfulness, Fairness, and Transparency:** Organizations must provide clear information about data collection and usage. Fairness, respect for the law and transparency are crucial in managing data (Mohan et al. 2019).
✓ **Purpose Limitation:** Data collection should occur only for specific, legitimate reasons and remain limited to those intentions (Rathnam, 2024).
✓ **Data Minimization:** The collection should be restricted to the data which is required to achieve the defined reason (Mohan et al. 2019).
✓ **Accuracy:** Organizations must verify the accuracy of the data regularly (Rathnam, 2024).
✓ **Storage Limitation:** Data storage duration should match necessity period, with secure erasure after use (Rathnam, 2024).
✓ **Integrity and Confidentiality:** Processing requires secure measures through technical and organizational protection systems (Mohan et al. 2019).
✓ **Accountability:** Data controllers must prove GDPR compliance (Rathnam, 2024).

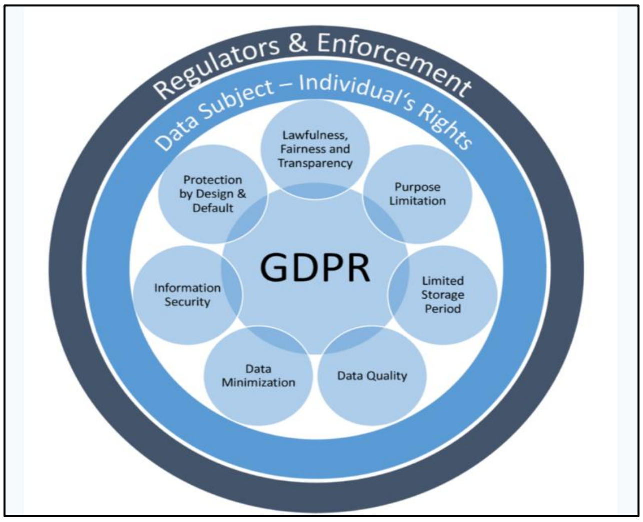


Fig 3 GDPR Regulation (Rathnam, 2024).

GDPR provides users with rights to control information: reviewing data, correcting inaccuracies, removal, data portability, objection for processing, and protection from automated decision-making without human intervention (Fakeyede, 2023).

- *Data Processing Agreements and Cross-Border Transfers:*

Data controllers must establish Data Processing Agreements (DPAs) with third-party cloud service providers handling data on their behalf (Fakeyede, 2023).

The GDPR requires these agreements outline: processing nature and purpose, data types and subjects, party obligations, and security measures (Rathnam, 2024).

Data transfers outside the EU are a major GDPR concern, requiring security measures like Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs), or specific derogations when transferring to countries without adequate protection laws. Organizations using cloud services must verify providers' GDPR compliance and their data storage locations and transfer protocols (Mohan et al. 2019).

➢ *Health Insurance Portability and Accountability Act (HIPAA):*

This act passed in 1996 by United States, functions to safeguard personal health information privacy and security. HIPAA existed before cloud computing became popular, yet it affects healthcare organizations and their cloud service providers who handle electronic protected health information (ePHI) (Maddali, 2024).

- *Scope and Applicability:*

HIPAA applies to two main categories of entities:

✓ **Covered Entities:** The law applies to healthcare providers (e.g., hospitals, clinics, doctors) and health plans (e.g., insurance companies) and healthcare clearinghouses that transmit health information electronically (Maddali, 2024).
✓ **Business Associates:** These are third-party vendors, such as cloud service providers, that perform functions involving access to ePHI on behalf of covered entities (Maddali, 2024).

A cloud vendor who stores or processes or transmits ePHI for a covered entity must be treated as a business associate and must follow HIPAA rules (Shah, 2023).

- *Key Rules and Requirements:*

HIPAA consists of multiple rules protecting health information privacy and security.

The Privacy Rule establishes standards for using and disclosing health information. It grants patients control through access, correction, and disclosure of accounting rights. Use of ePHI must be restricted to the minimum needed per purpose (Nosowsky & Giordano, 2006).

The Security Rule protects ePHI through administrative, physical and technical measures, requiring access controls, encryption, audit logs and authentication systems. Organizations must implement risk analysis to identify security vulnerabilities (Shah, 2023).

The Breach Notification Rule requires covered entities to inform affected individuals and HHS about ePHI breaches, establishing reporting timeframes and protocols (Maddali, 2024).

- *Business Associate Agreements (BAAs):*

The handling of ePHI by third parties requires covered entities to establish Business Associate Agreements (Shah, 2023). The BAA must specify authorized ePHI uses and impose protection requirements and establish notification procedures for breaches and enable both covered entities and HHS to conduct audits. The use of cloud providers for ePHI storage without a BAA constitutes a violation of HIPAA regulations (Nosowsky & Giordano, 2006).

- *Cloud-Specific Considerations Under HIPAA:*

Cloud computing systems present distinctive challenges for HIPAA compliance implementation.

✓ **Data Security:** Ensuring encryption of ePHI during transfer and storage (Shah, 2023).
✓ **Access Restrictions:** Limiting authorization and enforcing MFA (Shah, 2023).
✓ **Auditability:** Maintaining audit logs to trace ePHI access (Shah, 2023).
✓ **Data Backup:** Ensuring health data availability during outages (Shah, 2023).
✓ **Vendor Risk Management:** Vetting cloud vendors for HIPAA compliance (Shah, 2023).

Non-compliance with HIPAA regulations incurs penalties including maximum annual fines of $1.5 million per violation category and criminal prosecution for willful neglect. Healthcare organizations must maintain diligence when implementing cloud solutions (Maddali, 2024).

➢ *California Consumer Privacy Act (CCPA):*

This act was passed in 2018, enabling residents to control their personal information from 2020. The data governance regulations of the United States receive substantial impact from CCPA despite being a state-specific law affecting California-based businesses. The California Privacy Rights Act (CPRA) expanded CCPA provisions in 2023 (Maddali, 2024).

- *Scope and Applicability:*

CCPA applies to for-profit businesses collecting California residents' data meeting any threshold: Annual revenues over $25 million, having 100,000 consumers/households/devices when sharing personal information, or deriving half yearly revenue from selling consumer data. CCPA focuses on individual rights in commercial contexts, unlike GDPR or HIPAA regulations (Fakeyede, 2023).

- *Key Consumer Rights Under CCPA:*

The California Consumer Privacy Act gives residents data rights. CCPA's Right to Know enables access to personal information that businesses collect and sell. Individuals can request deletion of personal information from businesses. Through Right to Opt-Out, consumers can stop businesses from selling their data. CCPA protects against discrimination. CPRA added Right to Correct and Right to Limit Use of Sensitive Information (Yusuff, 2023).

- *Data Protection Requirements:*

CCPA imposes business obligations: Privacy policies must explain data collection and sharing. Companies must provide consumer data copies upon request. Consumers can sue businesses for unauthorized data access due to insufficient security. Vendor agreements must limit data use and uphold consumer rights (Yusuff, 2023).

- *Cloud Context:*

Businesses must establish management systems for cloud infrastructure. Data Mapping tracks consumer data location and flow. Access and deletion requests must be handled throughout cloud systems. Cloud vendors must demonstrate CCPA compliance through contracts and auditing (Harding et al., 2019).

- *Penalties and Enforcement:*

The CCPA enforcement rests with the California Attorney General and Privacy Protection Agency (CPPA). The maximum fine under CCPA reaches $2,500 per violation but rises to $7,500 when intentional. Consumers have a restricted right to sue when data breaches occur due to inadequate security practices (Harding et al., 2019).

IV. COMPLIANCE STRATEGIES IN THE CLOUD

Organizations that store sensitive data in cloud services must follow GDPR and HIPAA and CCPA regulations. Organizations need to implement a multi-layered compliance strategy when working with cloud infrastructure. Below Table.1 summarizes the challenges regarding data privacy and compliance in cloud (Kanungo, 2024).

➢ *Vendor Selection and Due Diligence:*

Selecting cloud service providers (CSPs) requires evaluation.

- Provider's compliance certifications (ISO 27001, SOC 2, FedRAMP, HITRUST).
- Security incident history.
- Support for regulatory requirements.
- Organizations need to evaluate the location of their data and service level agreements and incident response procedures. The contract should outline specific roles and responsibilities for all parties involved (Kanungo, 2024).

➢ *Data Encryption and Anonymization:*

Data encryption is essential for compliance. Organizations should implement.

- Encryption at rest and in transit.
- Secure key management with rotation.
- End-to-end encryption for sensitive data. Data anonymization helps meet legal obligations (Fayayola, 2024).

➢ *Access Control and Audit Trails:*

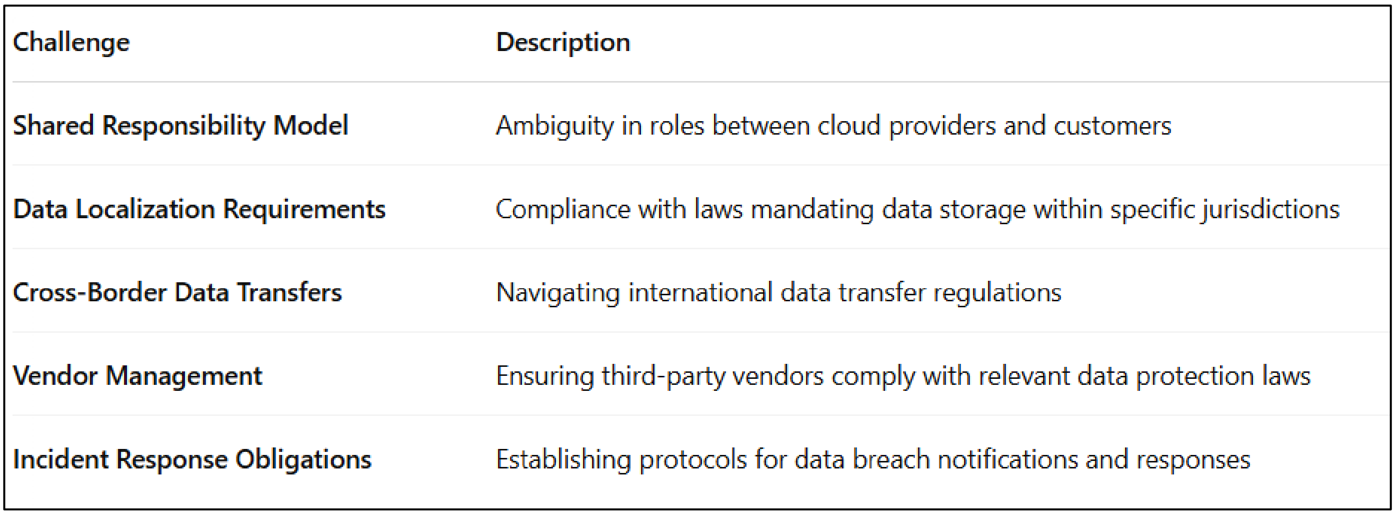
Organizations must introduce.

- Multi-factor authentication (MFA).
- Separation of duties.
- Role-based access control (RBAC) (Kanungo, 2024).

➢ *Incident Response Plans:*

Organizations need incident response plans including:

- Response roles and responsibilities.
- Communication procedures.
- Data containment protocols.
- Compliance with notification timelines.
- Regular testing ensures preparedness (Rathnam, 2024).



Challenge	Description
Shared Responsibility Model	Ambiguity in roles between cloud providers and customers
Data Localization Requirements	Compliance with laws mandating data storage within specific jurisdictions
Cross-Border Data Transfers	Navigating international data transfer regulations
Vendor Management	Ensuring third-party vendors comply with relevant data protection laws
Incident Response Obligations	Establishing protocols for data breach notifications and responses

Table 1 Challenges in Data Privacy and Compliance (Kanungo, 2024).

➢ *Regular Compliance Audits:*

Organizations should perform internal and third-party assessments to check their security controls and regulatory compliance. Audits reveal compliance gaps while generating evidence for regulatory compliance. These strategies help reduce risks and maintain customer trust (Pearson, 2010).

V. FUTURE VISION FOR PRIVACY AND COMPLIANCE IN CLOUD SYSTEMS

Data privacy in cloud computing evolves rapidly due to new regulations and AI-driven privacy management systems. The AI Act creates new directions for cloud security standards while establishing compliance requirements and allowing stakeholder participation throughout the AI lifecycle

(Gonzalez Torres & Sawhney, 2023). The regulation supports AI regulatory sandboxes and ML Ops to achieve compliance while supporting innovation. The framework supports testing automation pipelines for deploying AI services compliantly (Gonzalez Torres & Sawhney, 2023). Cloud compliance automation grows with AI and machine learning as primary drivers. Cloud security benefits from deep learning techniques providing anomaly detection and automation solutions (Alzoubi et al., 2024). Implementation faces challenges in data privacy, scalability and explainability. Future research will focus on algorithms meeting legal requirements while addressing these issues (Alzoubi et al., 2024). AI systems manage privacy functions in cloud environments, with real-time monitoring and automated processes improving security according to Banerjee (2024) and Gholami & Laure (2015). AI-driven solutions require attention to privacy concerns (Singh, 2023). Developing intelligent privacy management systems needs stakeholder collaboration and ethical guidelines (Dada et al., 2024).

VI. CONCLUSION

The data privacy and compliance landscape of cloud computing remains intricate as GDPR, HIPAA and CCPA safeguard user information. Strict regulations fail to ensure complete compliance as GDPR dark patterns remain widespread in privacy policies according to (Mohan et al. 2019). The e-commerce industry faces difficulties as cookies fail to meet lifecycle regulations, creating security vulnerabilities (Singh et al., 2024). GDPR and CCPA show commonalities yet operate through different enforcement systems (Bakare et al., 2024; Harding et al., 2019). The inconsistent regulatory framework demonstrates the need for worldwide data privacy standards. Healthcare must balance digital innovation with HIPAA and GDPR compliance requirements (Nosowsky & Giordano, 2006; Shah, 2023). Organizations must prioritize data privacy while navigating complex regulatory environments of cloud technologies. Organizations need proactive compliance strategies including privacy-by-design principles and monitoring of regulatory requirements. HIPAA regulations' effects on clinical research show the need to maintain innovation with compliance (Nosowsky & Giordano, 2006). The future requires global privacy standards and enhanced compliance education to ensure ethical data handling in cloud environments (Ehimuan et al., 2024; Fayayola et al., 2024).

REFERENCES

[1]. Samant, P. S. (2024). Leveraging AI for enhanced compliance with global data protection regulations in cloud computing environments. International Research Journal of Modernization in Engineering Technology and Science, 6(4). DOI: 10.56726/IRJMETS53514.

[2]. Fayayola, O., Olorunfemi, O., & Shoetan, P. (2024). DATA PRIVACY AND SECURITY IN IT: A REVIEW OF TECHNIQUES AND CHALLENGES. Computer Science & IT Research Journal, 5(3), 606–615. https://doi.org/10.51594/csitrj.v5i3.909

[3]. Maddali, R. (2024). AI-Powered Data Security Frameworks for Regulatory Compliance (GDPR, CCPA, HIPAA). International Journal of Engineering Technology Research & Management, Volume 08, Issue 04, ISSN: 2456-9348.

[4]. Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693–702). IEEE.

[5]. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4–5), 372–386.

[6]. Rathnam, L. (2024, April 2). GDPR – the challenges and the opportunity. Planet Compliance. https://www.planetcompliance.com/gdpr/gdpr-challenges-opportunity.

[7]. Thoom, S. R. (2025). Advances in data and AI governance: Navigating privacy, compliance, and trust. International Journal of Computer Engineering and Technology (IJCET), 16(1), 542-555.

[8]. Yusuff, M. (2023). Ensuring compliance with GDPR, CCPA, and other data protection regulations: Challenges and best practices. International Journal of Data Protection & Privacy Research.

[9]. Kanungo, S. (2024). Data privacy and compliance issues in cloud computing: Legal and regulatory perspectives. International Journal of Intelligent Systems and Applications in Engineering, 12(21s), 1721–1734.

[10]. Fakeyede, O. G., Okeleke, P. A., Hassan, A. O., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. International Journal of Research in Engineering and Science, 11(11), 184-192.

[11]. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57(5). https://doi.org/10.1007/s10462-024-10776-5.

[12]. Gonzalez Torres, A. P., & Sawhney, N. (2023). Role of Regulatory Sandboxes and ML Ops for AI-Enabled Public Sector Services. The Review of Socio-network Strategies, 17(2), 297–318. https://doi.org/10.1007/s12626-023-00146-y.

[13]. Banerjee, S. (2024). Intelligent Cloud Systems: AI-Driven Enhancements in Scalability and Predictive Resource Management. International Journal of Advanced Research in Science, Communication and Technology, 266–276. https://doi.org/10.48175/ijarsct-22840.

[14]. Dada, M., Daraojimba, O., Majemite, M., Nwokediegwu, Z., Obaigbena, A., & Oliha, J. (2024). Review of smart water management: IoT and AI in water and wastewater treatment. World Journal of Advanced Research and Reviews, 21(1), 1373–1382. https://doi.org/10.30574/wjarr.2024.21.1.0171.

[15]. Gholami, A., & Laure, E. (2015). Security and Privacy of Sensitive Data in Cloud Computing: A Survey of

Recent Developments. 131–150. https://doi.org/10.5121/csit.2015.51611.

[16]. Singh, N. (2023a). AI and IoT: A Future Perspective on Inventory Management. International Journal for Research in Applied Science and Engineering Technology, 11(11), 2753–2757. https://doi.org/10.22214/ijraset.2023.57200.

[17]. Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy (Vol. 11721, pp. 82–95). springer. https://doi.org/10.1007/978-3-030-33752-0_6

[18]. Singh, N., Do, Y., Yu, Y., Fouad, I., Kim, H., & Kim, J. (2024). Crumbled Cookies: Exploring E-commerce Websites? Cookie Policies with Data Protection Regulations. ACM Transactions on the Web. https://doi.org/10.1145/3708515

[19]. Harding, E. (Liz), Hannah Ji, L., Vanto, J. J., Ainsworth, S. C., & Clark, R. (2019). Understanding the scope and impact of the California Consumer Privacy Act of 2018. Journal of Data Protection & Privacy, 2(3), 234. https://doi.org/10.69554/tcfn5165

[20]. Bakare, S., Eneh, N., Adeniyi, A., & Akpuokwe, C. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. Computer Science & IT Research Journal, 5(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

[21]. Ehimuan, B., Akagha, O., Oguejiofor, B., Reis, O., & Ob, O. (2024). Global data privacy laws: A critical review of technology's impact on user rights. World Journal of Advanced Research and Reviews, 21(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

[22]. Shah, W. F. (2023). Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA. International Journal for Research in Applied Science and Engineering Technology, 11(8), 2189–2199. https://doi.org/10.22214/ijraset.2023.55551.

[23]. Nosowsky, R., & Giordano, T. J. (2006). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical Research. Annual Review of Medicine, 57(1), 575–590.https://doi.org/10.1146/annurev.med.57.121304.131257.