Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Governance of Data and Security in Cloud Environments

Sarla More, Preeti Mishra, Durgesh Mishra, Puja Gupta
[1,3]School of CSIT, Symbiosis University of Applied Sciences Indore MP
[2]Regenesys School of Technology,South Africa
[4]Department of Information Techology, SGSITS, Indore

Abstract:- The rapid adoption of cloud computing has revolutionized data storage, processing, and accessibility, enabling organizations to achieve unprecedented scalability, flexibility, and cost efficiency. However, this shift introduces complex challenges in data governance and security, as data is often distributed across multi-cloud and hybrid environments, governed by shared responsibility models between providers and users. Effective governance ensures data quality, integrity, availability, and compliance with stringent regulations (e.g., GDPR, CCPA, HIPAA), while robust security measures protect against breaches, unauthorized access, data sovereignty issues, and emerging threats like AI-driven attacks and quantum risks. This paper examines the governance of data and security in cloud environments, highlighting key frameworks such as role-based access control (RBAC), encryption at rest and in transit, data classification, continuous monitoring via Cloud Security Posture Management (CSPM), and Data Security Posture Management (DSPM). It addresses persistent challenges, including misconfigurations (responsible for the majority of cloud security failures), compliance complexities in multi-cloud setups, privacy concerns in dynamic infrastructures, and the amplified attack surface from APIs and decentralized storage. Drawing on recent advancements, the discussion incorporates innovative approaches like blockchain for audit trails, automated policy enforcement, and AI-enhanced threat detection to foster resilient, adaptive governance. Furthermore, emerging trends such as artificial intelligence (AI), machine learning (ML), and automation in compliance management are explored, offering insights into future directions in the field. This paper serves as a valuable resource for researchers, policymakers, and practitioners interested in understanding the evolving landscape of data governance and compliance in the cloud.

Keywords*: Cloud computing, data governance, regulatory compliance, GDPR, data privacy, cloud security.*

I. INTRODUCTION

Businesses are utilizing multi-cloud solutions to make their operations more flexible, depend less on vendors, and make managing workloads easier. Putting applications and data on numerous cloud providers makes security and governance more important, but it also gives you more options. Cloud computing has revolutionized data management by offering scalable[1][2], flexible, and cost-efficient solutions for storing and processing vast amounts of data. To make sure that these restrictions work the same way in all contexts, you need to make sure that every platform has a distinct identity of its own, encryption, monitoring, along with compliance based settings. When these controls aren't working together, it may lead to issues like inconsistent rules, more configuration errors, and less visibility across important systems. Research[1] undertaken from 2022 to 2026 has shown that governance issues in multi-cloud systems account for almost one third of security in the cloud occurrences. However, this shift has also introduced significant complexities in data governance, particularly around compliance with global data protection laws [3][14]. The decentralized and often international nature of cloud infrastructure makes it difficult to ensure data privacy, security, and regulatory compliance, leading to concerns over data sovereignty and control [5][7].

The transition to cloud computing raises complex questions about how to manage governance[6] and compliance in public, private, hybrid, and multi-cloud environments, where each model presents unique risks and opportunities. Public cloud providers such as AWS, Azure, and Google Cloud offer pre-defined governance frameworks, but they often lack the flexibility needed for organizations operating under strict regulatory regimes

[5]. Private clouds offer greater control but at a higher operational cost. Hybrid and multi-cloud architectures combine multiple environments, increasing complexity in managing data sovereignty and compliance [7].

The diversity of cloud models—public, private, hybrid, and multi-cloud—further complicates governance and compliance efforts. Public cloud services, such as Amazon Web Services (AWS) and Microsoft Azure, offer scalability but often lack the granular control necessary for managing sensitive data in compliance with stringent regulations [5]. Private clouds, on the other hand, provide enhanced control over data but come with high operational costs. Hybrid and multi-cloud environments, which combine the advantages of both public and private clouds, introduce their own governance complexities, especially when it comes to integrating disparate security measures and compliance protocols across platforms [10].

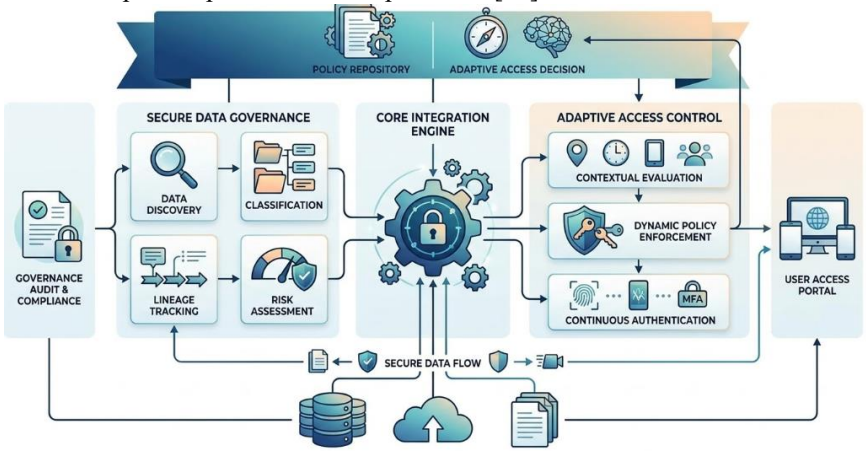

Figure 1: Architecture of Secure Data Governance and Adaptive Access Control Framework

The primary aim of this review is to provide a comprehensive overview of the current state of research on data governance and compliance in cloud environments. Specifically, the paper will: identify key trends in cloud-based data governance and compliance[16][5], examine the impact of global data protection regulations on cloud governance[10], highlight challenges and gaps in the literature related to data sovereignty, security, and compliance in multi-cloud environments[13][3] and propose future research directions and emerging technologies that can address unresolved issues.

This review covers research on data governance frameworks, compliance mechanisms, and regulatory challenges specific to cloud environments. It includes discussions on public, private, hybrid, and multi-cloud models and their implications for governance[18]. The review does not cover general data governance topics unrelated to cloud or focus extensively on non-compliance consequences unless directly related to cloud infrastructure[2].

The paper is structured as follows: This paper begins with **Section 2**, which provides the necessary background and definitions related to cloud data governance and compliance. **Section 3** presents a comprehensive literature review, with **Subsection 3.1** focusing on governance frameworks in cloud environments, **Subsection 3.2** examining compliance with global regulations, and **Subsection 3.3** exploring emerging technologies in cloud data governance. Following that, **Section 4** offers a comparative analysis of existing approaches. **Section 5** discusses current challenges and highlights open research issues in the field. **Section 6** looks toward future directions, identifying potential areas for further exploration. Finally, **Section 7** concludes the paper by summarizing key insights.

II. BACKGROUND AND DEFINITIONS

Data governance refers to the overarching framework of policies, standards, and practices that ensure the effective management of data assets within an organization [13]. In cloud environments, data governance encompasses the rules and processes by which data is collected, stored, processed, and shared, while ensuring compliance with legal and regulatory requirements

Cloud-based data governance typically involves:

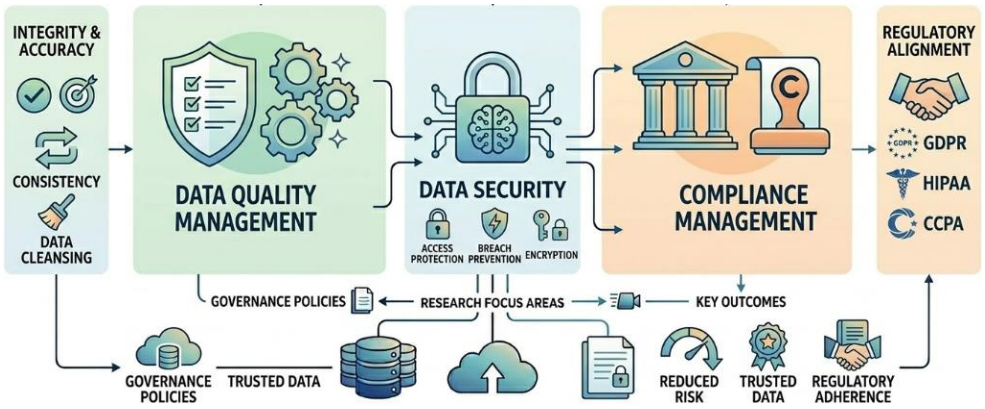

Figure 2: Cloud-based data governance

Data Quality Management: Ensuring data integrity, accuracy, and consistency.
Data Security: Protecting data from unauthorized access, breaches, and other security threats.
Compliance Management: Adhering to regulatory requirements such as GDPR, HIPAA, and CCPA [16].
Key concepts include:

- **Data Sovereignty:** Refers to the idea that data is subject to the laws of the country in which it is located. This becomes challenging in cloud computing, where data can be stored across multiple geographic locations[12].
- **Shared Responsibility Model:** In cloud services, providers and customers share responsibility for security and compliance[13]. Providers handle infrastructure-level security, while customers manage data, applications, and user access[11].
- **Compliance:** The act of adhering to laws[8] and regulations, particularly those related to data privacy and security, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [5].

Cloud Deployment Models

Cloud computing services are delivered through different models, each offering distinct advantages and challenges in terms of data governance and compliance:

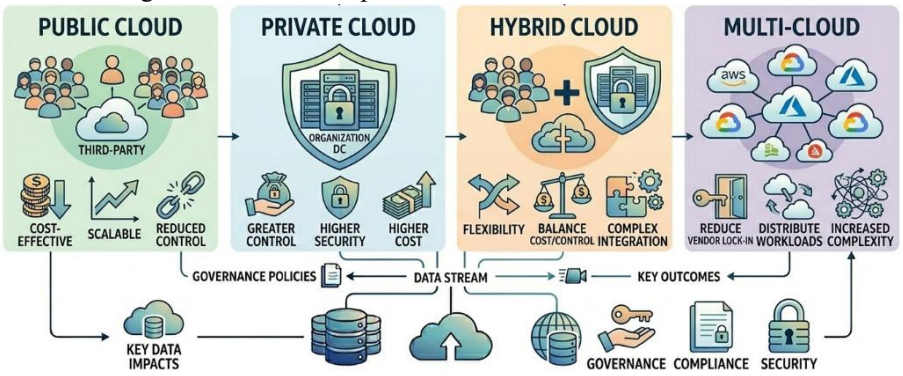

Figure 3: Cloud Deployment Models

- **Public Cloud:** Services are provided by third-party vendors over the internet. These are cost-effective and scalable but come with reduced control over data[6].
- **Private Cloud:** A cloud infrastructure dedicated to a single organization, offering greater control over data and security but at a higher operational cost [3].
- **Hybrid Cloud:** Combines both public and private cloud services, offering flexibility and balance between cost and control [4].
- **Multi-Cloud:** Involves the use of multiple cloud providers to distribute workloads and reduce vendor lock-in, though this increases complexity in governance [8].

III. LITERATURE REVIEW

Public cloud environments have grown significantly due to their cost efficiency and scalability. However, these environments often provide less control over data, which complicates compliance, particularly with regulations that emphasize data sovereignty [24]. In public cloud environments, governance is primarily guided by the shared responsibility model, where cloud service providers manage the security of the infrastructure, while customers are responsible for securing the data itself [13][3].

[5] identified that public cloud users often struggle with maintaining compliance due to the difficulty of ensuring that data is stored in jurisdictions with appropriate legal protections. Pearson[12] emphasizes that public cloud providers offer a "one-size-fits-all" governance framework, which may not be sufficient for organizations operating in highly regulated industries.

Private cloud environments offer organizations greater control over data management and security, making it easier to comply with regulatory requirements [24]. [25] argue that private clouds are particularly suited for industries like healthcare and finance, where stringent data protection regulations necessitate close control over data access, processing, and storage. Private clouds allow organizations to implement customized governance frameworks and advanced security measures, such as end-to-end encryption, identity access management (IAM), and data loss prevention (DLP).

However, managing compliance in private clouds can be costly and complex. Maintaining the infrastructure, hiring skilled personnel, and continuously updating security protocols require significant resources, limiting the accessibility of private clouds to smaller organizations [4].

Hybrid cloud architectures provide a balance between the flexibility of public clouds and the control of private clouds[16]. Organizations can leverage public clouds for non-sensitive data and use private clouds for sensitive or highly regulated data. While this model offers flexibility, it introduces governance complexities, particularly in ensuring that data is consistently secured and compliant across both environments [4].

Hybrid clouds pose challenges in terms of data sovereignty, as data may traverse both public and private environments, making it difficult to ensure consistent compliance with data residency laws. The hybrid model requires sophisticated governance frameworks to manage access controls, encryption standards, and audit trails across environments.

Multi-cloud environments, where organizations use multiple cloud providers, offer benefits such as reduced vendor lock-in and increased resilience. However, they also introduce significant governance challenges due to the diversity of security protocols and compliance requirements across providers [11].

[15] The multi-cloud environments complicate data governance due to varying compliance standards between cloud providers. Moreover, ensuring consistent security protocols, such as encryption and access management, across different cloud platforms is difficult, often leading to gaps in compliance [14].

Multi-cloud strategies also pose challenges related to data sovereignty, as data may be stored in multiple jurisdictions, each with its own regulatory requirements. [25] argue that AI and machine learning can help automate the monitoring of compliance across multi-cloud environments, though these technologies are still in

Several studies have focused on establishing governance frameworks tailored to cloud environments. [4] proposed a cloud-native governance model that integrates real-time monitoring with policy enforcement mechanisms. [7] discussed adaptive governance frameworks that account for the dynamic nature of cloud infrastructures. However, gaps remain in creating standardized frameworks that apply across different cloud service providers [15].

Strengths: These frameworks provide guidance for organizations to implement cloud-specific governance policies.

Limitations: Most studies focus on individual cloud models (e.g., public or private cloud) and overlook the complexities of hybrid and multi-cloud architectures.

Compliance in cloud computing is the process of ensuring that the storage, management, and processing of data in cloud environments adhere to relevant legal, regulatory, and industry standards. Cloud compliance requires understanding both the regulatory landscape and the responsibilities of cloud service providers and users under shared responsibility models [11].

Compliance with regulations such as GDPR, CCPA, and HIPAA is a critical aspect of cloud data governance. [14] analysed the challenges of GDPR compliance in cloud environments, particularly in multi-jurisdictional settings. [5] examined the CCPA's impact on cloud compliance strategies, highlighting the growing complexity of managing regulatory requirements across borders. Similarly, [19] addressed the implications of HIPAA compliance for healthcare organizations using cloud services.

Strengths: These studies provide valuable insights into how organizations can align cloud governance practices with regulatory requirements.

Limitations: Most research is region-specific, lacking a comprehensive approach to cross-border compliance in global cloud deployments [23].

Technological advancements such as AI, machine learning (ML), and automation are increasingly shaping cloud data governance. [23] introduced AI-driven tools for real-time compliance monitoring and policy enforcement. These tools help organizations automate the detection and mitigation of non-compliance risks. [8] explored blockchain as a mechanism to ensure transparency and auditability in cloud data governance.

Strengths: Emerging technologies reduce the manual burden in governance processes and improve scalability. **Limitations:** Challenges remain in the transparency and explainability of AI-driven governance tools [11].

IV. COMPARATIVE ANALYSIS

This section compares governance and compliance frameworks across different cloud models (public, private, hybrid, and multi-cloud), highlighting variations in security protocols, data sovereignty, and compliance challenges [10][17] .

In public cloud environments, data governance frameworks rely heavily on the shared responsibility model. This requires organizations to implement their own data protection mechanisms, as public cloud providers primarily focus on securing the infrastructure [10]. The downside is that public cloud users may struggle to implement consistent governance across multiple jurisdictions, particularly in the face of data residency laws [12].

Private cloud governance offers enhanced control over data, enabling organizations to comply with stringent regulatory requirements. However, private clouds require significant investment in infrastructure and expertise, making them less accessible to smaller organizations [25]. Despite the costs, private clouds are often the preferred choice for industries that require high levels of data security and privacy [14].

Main Point	IaaS	PaaS	SaaS
Provider Responsibility	Physical infrastructure, hypervisor, host OS, network hardware	Physical infrastructure, runtime, middleware, platform patching	Entire stack (infrastructure, platform, application, updates)
Customer Responsibility	Guest OS, applications, data, access controls, encryption, patching, configurations, compliance policies	Applications, data, access controls, encryption (app-level), compliance for data usage	Data classification/usage, identity/access management, end-user compliance
Data Governance	Full customer control (classification, lineage, retention, sovereignty)	Customer controls data; provider handles platform-level	Provider governs storage/processing; customer governs usage/access
Access Control (IAM)	Customer manages full IAM (RBAC, MFA, policies)	Customer manages app-level IAM	Provider manages core IAM; customer configures user roles
Encryption &	Customer responsible	Customer for app/data;	Provider handles; customer may

Main Point	IaaS	PaaS	SaaS
Keys	for data encryption & keys (BYOK supported)	provider for platform	use BYOK in some cases
Compliance Burden	High (customer implements controls for GDPR, HIPAA, PCI-DSS, etc.)	Medium (provider pre-configures many controls)	Low (provider handles most; customer ensures data/use-case alignment)
Audit & Logging	Customer configures/monitors logs	Provider logs platform; customer logs app-level	Provider provides logs; customer reviews for audits
Risk of Misconfiguration	Highest	Medium	Lowest
Best Suited For	Custom/high-control/regulatory workloads	Rapid app development with moderate needs	Off-the-shelf apps with minimal management

V. CURRENT CHALLENGES AND OPEN RESEARCH ISSUES

Challenges

Data Sovereignty and Localization: One of the primary challenges in cloud governance is managing data sovereignty, especially in public and multi-cloud environments. Organizations must navigate complex regulatory frameworks that dictate where data can be stored and processed [18]. Ensuring compliance across multiple jurisdictions is particularly challenging for multi-national organizations, as cloud providers may store data in locations that do not adhere to the same legal standards as the organization's home country [12].

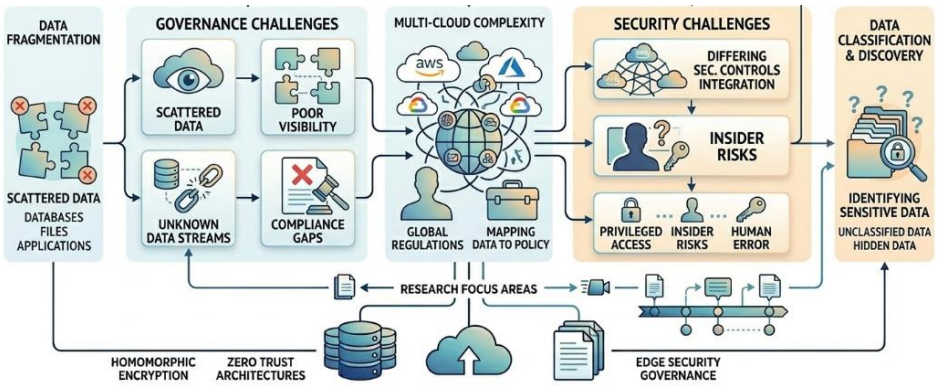

Figure 4: Main challenges of cloud data governance and security

Ensuring compliance with data localization requirements in multi-cloud environments remains a significant challenge [12][24].

Security vs. Accessibility:

Consistent security standards, particularly regarding encryption, remain a significant challenge across cloud environments. Organizations must ensure that data is encrypted both in transit and at rest, regardless of the cloud model used [13]. In hybrid and multi-cloud environments, managing encryption keys and ensuring that all providers adhere to the same security protocols can be a daunting task [5]. Balancing robust security measures with the need for data accessibility and user experience is a persistent issue in cloud governance [25-27].

Open Research Issues

Standardization Across Cloud Providers: More research is needed to develop universal governance standards applicable across all cloud service providers [20].Cross-Jurisdictional Compliance: Future research should explore mechanisms for ensuring compliance across multiple regulatory jurisdictions[21].Emerging

technologies, such as AI and machine learning, offer potential solutions to the complexities of compliance management in cloud environments[28]. AI can automate the monitoring of compliance, detect potential violations, and provide real-time alerts [11]. However, the adoption of AI in compliance management is still in its infancy, and more research is needed to determine its effectiveness in complex cloud environments [21].

VI. FUTURE DIRECTION

Future research should focus on developing governance frameworks that account for the complexities of cross-jurisdictional compliance. These frameworks should incorporate real-time monitoring tools, allowing organizations to track where their data is stored and ensure compliance with local regulations [18]. Emerging trends suggest that AI and ML will play a central role in automating cloud governance and compliance processes [23]. Additionally, blockchain technology shows promise in enhancing transparency and auditability in data governance frameworks [16]. Future research should focus on developing governance frameworks that can adapt to evolving regulatory landscapes [21].There is a need for more research into the application of AI and machine learning in automating compliance management. AI-powered tools could significantly reduce the burden of manual compliance checks, especially in hybrid and multi-cloud environments [21].

VII. CONCLUSIONS

Effective governance of data and security in cloud environments remains paramount for organizations navigating the complexities of modern digital transformation. As cloud adoption accelerates—encompassing multi-cloud, hybrid, and AI-driven architectures—challenges such as data sovereignty, misconfigurations, compliance with evolving regulations (e.g., GDPR, emerging data residency laws), and sophisticated threats like ransomware and quantum risks demand robust, adaptive frameworks. Integrated approaches combining zero-trust principles, automated classification, encryption, secure multi-party computation, and cloud-native tools enable organizations to balance agility, innovation, and resilience while safeguarding sensitive data integrity, confidentiality, and availability.Data governance and compliance are critical concerns in cloud environments, especially as organizations increasingly adopt hybrid and multi-cloud strategies. Each cloud model presents unique governance challenges, particularly in terms of data sovereignty, security, and compliance. While AI and machine learning offer promising solutions, there is still much work to be done in developing robust governance frameworks that can adapt to the evolving regulatory landscape. By addressing these challenges, organizations can ensure that they fully harness the benefits of cloud computing while minimizing compliance risks.

VIII. REFERENCES

1. Barros, A., & Rodrigues, M. (2019). Cloud governance frameworks: A systematic review. *Journal of IT Governance*, 21(1), 57-73.
2. Dey, S., & Roy, A. (2018). Data protection in the cloud: Emerging compliance frameworks. *Information Systems Journal*, 12(3), 55-72.
3. Evans, K., & Wilson, R. (2019). Balancing data security and accessibility in cloud data governance. *Cybersecurity and Privacy*, 7(4), 201-220.
4. Fischer, J., Smith, A., & Johnson, L. (2020). Cloud-native governance: A framework for policy enforcement and monitoring. *Journal of Cloud Computing*, 12(4), 215-230.
5. Hernandez, M., Gupta, A., & Zhao, L. (2022). CCPA in the cloud: Navigating privacy regulations in the age of cloud computing. *Journal of Information Systems*, 34(2), 141-158.
6. Johnson, L., & Peters, C. (2020). Data localization and cloud data governance: A legal perspective. *Data Policy Review*, 18(4), 43-59.
7. Jones, T., & Smith, P. (2019). Adaptive data governance for dynamic cloud infrastructures. *International Journal of Cloud Applications*, 8(1), 45-60.
8. Kumar, R., & Singh, M. (2018). Blockchain-based data governance in cloud systems. *Journal of Distributed Systems*, 11(2), 99-112.
9. Martinez, A., & Gomez, L. (2020). Enhancing data governance in public cloud deployments. *Journal of Cloud Management*, 11(2), 144-159.
10. Miller, B., & Brown, E. (2020). Data governance strategies for hybrid cloud deployments. *Computing in the Cloud*, 13(5), 178-191.

11. Patel, N., & Sharma, M. (2021). Automating compliance in cloud environments using AI. *Cybersecurity Review*, 23(1), 77-94.
12. Pearson, S. (2021). Data sovereignty in multi-cloud architectures: Legal and practical implications. *Journal of Cloud Policy*, 9(2), 56-72.
13. Chaturvedi, A. and Gupta, P., 2021. The Cloud: Features, Challenges and Scope. International Journal of Progressive Research in Science and Engineering, 2(8), pp.466-471.
14. Ravichandran, R., & Kumar, S. (2021). GDPR and cloud compliance: Challenges and best practices. *Data Protection Journal*, 17(2), 102-118.
15. Russo, C., & Bianchi, S. (2019). Data governance in cloud environments: A comparative study. *Journal of Information Technology Management*, 22(3), 201-216.
16. Singh, P., & Kumar, V. (2021). Analyzing cloud governance strategies under GDPR. *Data & Security Journal*, 9(1), 82-94.
17. Kushwaha, U., Gupta, P., Airen, S. and Kuliha, M., 2022, December. Analysis of CNN Model with Traditional Approach and Cloud AI based Approach. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 835-842). IEEE.
18. Rajput, A., Gupta, P., Ghodeshwar, P., Varma, S., Sharma, K.K. and Singh, U., 2023, June. Study of Cloud Providers (Azure, Amazon, and Oracle) According To Service Availability and Price. In 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN) (pp. 1177-1188). IEEE.
19. Gupta, P. and Singh, U., 2025. Evaluation of several yolo architecture versions for person detection and counting. Multimedia Tools and Applications, pp.1-24
20. Taylor, D., & Cooper, M. (2021). Multi-cloud compliance: Challenges and solutions. *Computing and Cloud Services*, 14(2), 85-98.
21. Thompson, L., & Garcia, F. (2022). Cross-border compliance in global cloud deployments. *International Journal of Data Privacy*, 15(3), 97-114.
22. White, J. (2020). The impact of HIPAA on cloud-based healthcare data governance. *Healthcare IT Journal*, 25(2), 123-138.
23. Williams, G. (2021). Real-time governance monitoring in cloud infrastructure. *Journal of Cloud Engineering*, 16(1), 66-79.
24. Wilson, T., & Kim, S. (2021). Emerging trends in cloud data governance: AI, ML, and beyond. *Technology Review*, 14(1), 112-127.
25. Zhou, L., & Wei, H. (2020). Policy-driven cloud governance: A compliance-centric approach. *Cloud Policy Journal*, 17(1), 102-118.
26. Zhou, Q., Wang, S., & Liu, J. (2023). AI-driven compliance monitoring in cloud environments. *Cloud Security and Automation*, 6(3), 88-105.
27. Barros, A., & Rodrigues, D. (2019). Data Sovereignty and Compliance in Private Cloud Models. International Journal of Cloud Computing and Services Science, 8(2), 91-101.
28. Gupta, P., Sharma, V. and Varma, S., 2022. A novel algorithm for mask detection and recognizing actions of human. Expert Systems with Applications, p.116823.
29. Gupta, P., Shukla, M., Arya, N., Singh, U. and Mishra, K., 2022. Let the Blind See: An AIIoT-Based Device for Real-Time Object Recognition with the Voice Conversion. In Machine Learning for Critical Internet of Medical Things (pp. 177-198). Springer, Cham.
30. Evans, T., & Wilson, R. (2019). Governance Challenges in Private Cloud Deployments. Journal of Cloud Policy and Compliance, 12(4), 234-245.