ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

CYBERSECURITY IMPLICATIONS OF WEAK DATA GOVERNANCE IN CLOUD-BASED DATABASES: A COMPARATIVE STUDY

Bharath Kishore Gudepu
Developer 4, Systems Software
Kemper, Dallas, TX, USA
email: bharathetl93@gmail.com

Praveen Kumar Pemmasani
Sr. Network Architect
City of Dallas, Dallas, TX, USA
email: pk.pemmasani@gmail.com

Krishna Chaitanya Gonugunta
Sr Database Administrator
NSHE, Nevada, USA
email: krishna.gonugunta@gmail.com

ABSTACT:
As organizations increasingly migrate to cloud-based databases, ensuring data security has become a paramount concern. This study explores the cybersecurity implications of weak data governance in cloud environments through a comparative analysis of 30 organizations across the healthcare, finance, and e-commerce sectors. Using a mixed-methods approach, the study evaluates Governance Effectiveness Scores (GES) alongside Cybersecurity Incident Scores (CIS), incident response times, and breach frequencies. The findings reveal a strong negative correlation between governance maturity and cybersecurity risk, with weak governance significantly increasing vulnerability to threats such as unauthorized access, misconfigurations, and ransomware. Regression analysis further confirms that governance effectiveness is a critical predictor of cybersecurity outcomes, even when controlling for industry, cloud provider, and regulatory compliance. Visual tools such as radar charts and heatmaps illustrate the disparity in governance dimensions and incident profiles. The study highlights the urgent need for organizations to treat data governance as a strategic imperative, emphasizing its role in reducing risk, improving resilience, and ensuring regulatory compliance in cloud environments.
Keywords: Cybersecurity, Data Governance, Cloud-Based Databases, Incident Response, Data Breaches, Risk Mitigation, Compliance

Introduction

Background and context

The exponential growth of cloud computing has revolutionized data storage, access, and management for organizations worldwide (Naik, 2023). Cloud-based databases, offering scalability, flexibility, and cost-efficiency, have become the backbone of modern enterprise IT infrastructures. However, the rapid transition to cloud environments has also introduced significant cybersecurity vulnerabilities, particularly when data governance frameworks are weak or poorly implemented. Weak data governance often results in the mishandling of sensitive

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

information, insecure access controls, and a lack of regulatory compliance, making cloud databases prime targets for cyberattacks (Ahmad et al., 2021). Inadequate governance mechanisms compromise data integrity, availability, and confidentiality-cornerstones of cybersecurity-thus raising alarm across industries that handle sensitive or regulated data.

Relevance of data governance in the cloud

Data governance refers to the formal management of data availability, usability, integrity, and security within an organization (Alabi, 2023). In cloud environments, governance becomes even more complex due to the shared responsibility model, in which both cloud service providers (CSPs) and customers have roles in securing data assets. Weaknesses in governance manifest in several ways- such as inconsistent metadata standards, unclassified data, poor role-based access controls, and inadequate audit mechanisms (Thompson et al., 2025). These weaknesses expose organizations to data breaches, insider threats, ransomware attacks, and legal penalties due to non-compliance with data protection regulations like GDPR, HIPAA, or India's DPDP Act. Thus, ensuring robust governance protocols in cloud settings is no longer a luxury but a critical necessity for cybersecurity resilience.

Emerging threat landscape and cloud-specific vulnerabilities

The cybersecurity threat landscape has become increasingly sophisticated, with threat actors exploiting cloud-specific vulnerabilities such as misconfigured storage buckets, insecure APIs, lack of encryption, and shadow IT deployments. In environments with weak data governance, these vulnerabilities are magnified (Parn & Edwards, 2019). For instance, a misconfigured access policy in a cloud database without proper governance oversight can lead to unauthorized access or data exfiltration. Furthermore, multi-tenant cloud architectures pose additional challenges, where inadequate isolation between clients could result in lateral movement of threats (Del Piccolo et al., 2016). Weak governance fails to provide the oversight needed to monitor, detect, and respond to these incidents in a timely manner.

Comparative study rationale

This research undertakes a comparative analysis of organizations with strong versus weak data governance frameworks in cloud-based environments to assess the correlation between governance maturity and cybersecurity performance (Kouatli, 2014). By examining case studies, audit reports, and incident data from sectors such as healthcare, finance, and e-commerce, the study evaluates how lapses in governance directly influence the frequency, impact, and nature of cybersecurity incidents (Mishra et al., 2022). This comparison aims to illuminate best practices, highlight risk-prone patterns, and provide actionable recommendations for mitigating threats through enhanced governance policies.

Research gap and objectives

Despite growing discourse on cloud security, there is limited empirical research linking weak data governance directly to cybersecurity outcomes in cloud-based databases. Most studies either focus exclusively on technical vulnerabilities or treat governance as a secondary concern. This research fills that gap by positioning data governance at the forefront of cybersecurity strategy in cloud contexts. The objectives are to (1) identify specific governance failures that lead to cybersecurity breaches, (2) compare the breach incidence rate between governance-mature and governance-weak organizations, and (3) propose a governance model optimized for cloud database security. The study thus contributes to the emerging dialogue on how holistic, policy-

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

driven approaches can complement technical defenses in securing cloud data infrastructures.

Methodology

Research design and approach

This study adopts a mixed-methods comparative research design to evaluate the cybersecurity implications of weak data governance in cloud-based databases. The research combines qualitative case studies and quantitative statistical analysis to provide a comprehensive understanding of how governance maturity levels affect cybersecurity outcomes. A comparative cross-sectional analysis was performed across three major sectors—healthcare, finance, and e-commerce—owing to their data-intensive operations and regulatory sensitivity. Both primary and secondary data were utilized to ensure triangulation and validation of findings.

Sample selection and data sources

A purposive sampling strategy was used to select 30 organizations (10 from each sector), categorized based on the maturity of their data governance practices: 15 with strong governance frameworks and 15 with weak or non-standardized frameworks. Governance maturity was assessed using a modified Data Governance Maturity Model (DGMM), considering dimensions such as data quality, stewardship, access control, metadata management, policy enforcement, and audit readiness. Sources of data included organizational security audit reports, governance policy documents, incident response logs, compliance assessments, and structured interviews with Chief Information Security Officers (CISOs) and data protection officers.

Cybersecurity metrics and incident profiling

Cybersecurity effectiveness was evaluated using key indicators such as the number of data breaches, nature and vector of attacks (e.g., SQL injection, misconfigured storage, access control violations), incident response time, and recovery costs. These metrics were extracted from publicly available databases (e.g., Verizon Data Breach Investigations Report, ENISA Threat Landscape) and corroborated with anonymized incident reports provided by participating organizations. A standardized Cybersecurity Incident Scoring (CIS) system was developed to normalize incident severity across different organizations and sectors.

Governance assessment tools

A structured governance audit checklist, based on ISO/IEC 38505 and NIST SP 800-53, was used to evaluate the comprehensiveness of data governance in each organization. The checklist covered domains such as data classification, encryption policies, identity and access management (IAM), third-party risk management, and compliance tracking mechanisms. Each organization was assigned a Governance Effectiveness Score (GES) ranging from 0 to 100, which was later used as a continuous variable in correlation and regression analyses.

Experimental design and statistical analysis

The study employed inferential statistical techniques to examine the relationship between data governance effectiveness and cybersecurity performance. Pearson's correlation coefficient was used to test the strength and direction of the relationship between GES and CIS across the sample. Further, an independent samples t-test was conducted to compare the mean cybersecurity incident scores between governance-strong and governance-weak organizations. To control for sectoral variability, a multivariate regression analysis was performed with control variables including organization size, cloud service provider type (e.g., AWS, Azure, Google Cloud), and regulatory environment (e.g., GDPR, HIPAA, PCI DSS). A significance threshold of $p < 0.05$ was used in

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

all statistical tests.

Qualitative content analysis

The structured interviews with security leaders were transcribed and thematically analyzed using NVivo software to identify recurring patterns related to governance failures, threat awareness, and cloud-specific risks. These qualitative insights were integrated with the quantitative findings to enrich the interpretation of results and provide sector-specific recommendations.

Ethical considerations

All data collection procedures adhered to ethical standards, with informed consent obtained from all participants. Sensitive data were anonymized, and confidentiality agreements were signed where necessary. The study was approved by the institutional ethics committee, and strict data handling protocols were followed throughout the research process.

Limitations and delimitations

The study is limited to three sectors and a sample of 30 organizations, which may not fully capture global variability in governance practices. Additionally, reliance on self-reported governance scores and cybersecurity incidents introduces a potential bias, which was mitigated through triangulation and validation with external datasets.

Results

The comparative analysis of cybersecurity implications across organizations with varying levels of data governance maturity revealed significant trends. As presented in Table 1, organizations with strong data governance frameworks consistently demonstrated lower cybersecurity incident scores (CIS) and fewer data breaches per year compared to those with weak governance. For instance, in the finance sector, organizations with strong governance had an average CIS of 1.7 and just 0.8 breaches per year, whereas weakly governed counterparts had a CIS of 6.9 and 3.7 breaches annually. This pattern was similarly evident across the healthcare and e-commerce sectors.

Table 1: Governance Effectiveness Score (GES) and Cybersecurity Incident Score (CIS) by sector

Sector	Governance category	No. of Orgs	Avg. GES (0–100)	Avg. CIS (0–10)	Avg. Breaches/Year
Healthcare	Strong Governance	5	87.2	2.1	1.2
Healthcare	Weak Governance	5	41.3	7.3	4.6
Finance	Strong Governance	5	90.6	1.7	0.8
Finance	Weak Governance	5	38.7	6.9	3.7
E-commerce	Strong Governance	5	84.5	2.5	1.6
E-commerce	Weak Governance	5	43.2	7.8	5.1

The correlation analysis in Table 2 further supports these observations, showing a strong negative

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

correlation between Governance Effectiveness Score (GES) and CIS ($r = -0.82$, $p < 0.01$), as well as between GES and average breaches per year ($r = -0.75$, $p < 0.01$). Moreover, organizations with higher GES tended to have significantly faster incident response times, as indicated by a negative correlation ($r = -0.71$, $p < 0.01$), underscoring the operational benefits of strong governance practices.

Table 2: Pearson Correlation Matrix – governance and cybersecurity metrics

Variable	GES	CIS	Breaches/Year	Response Time (hrs)
GES	1.00	-0.82	-0.75	-0.71
CIS	-0.82	1.00	0.79	0.68
Breaches/Year	-0.75	0.79	1.00	0.58
Response Time (hrs)	-0.71	0.68	0.58	1.00

All correlations significant at $p < 0.01$

Statistical validation through an independent samples t-test, shown in Table 3, confirmed that the differences between governance-strong and governance-weak groups were highly significant. Organizations with robust governance frameworks had an average CIS of 2.1, compared to 7.3 in weak governance setups ($t = -22.6$, $p < 0.001$). Similarly, response times and breach frequencies were significantly lower in governance-strong environments, highlighting the tangible security advantage of effective data governance.

Table 3: Independent Samples t-test – Strong vs. Weak governance

Metric	Strong governance (Mean ± SD)	Weak governance (Mean ± SD)	t-value	p-value
Cybersecurity Incident Score (CIS)	2.1 ± 0.4	7.3 ± 0.5	-22.6	<0.001
Avg. Breaches/Year	1.2 ± 0.5	4.5 ± 1.1	-7.9	<0.001
Response Time (hrs)	6.5 ± 2.3	18.4 ± 3.1	-9.4	<0.001

The multivariate regression results in Table 4 revealed that governance effectiveness ($\beta = -0.61$, $p < 0.001$) was the most significant predictor of cybersecurity incident scores, even after controlling for cloud service provider type, industry sector, and compliance status. Interestingly, compliance with regulatory frameworks such as GDPR and HIPAA also showed a moderate negative influence on incident scores ($\beta = -0.26$, $p = 0.002$), suggesting that policy adherence strengthens governance posture.

Table 4: Multivariate Regression – Predictors of Incident Score (CIS)

Predictor Variable	β (Standardized Coefficient)	Std. Error	t-value	p-value
Governance Effectiveness Score (GES)	-0.61	0.09	-6.78	<0.001
Cloud Provider (AWS ref.)	Azure: 0.14, GCP: 0.18	0.07	1.85	0.072
Sector (Finance ref.)	Healthcare: 0.09, E-commerce: 0.12	0.06	1.35	0.192
Compliance Status (Yes=1)	-0.26	0.08	-3.25	0.002

Visual evidence is provided in Figure 1, where a radar chart illustrates the disparity in

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

performance across governance dimensions between strong and weak governance organizations. Key areas such as data classification, encryption standards, and audit readiness exhibited stark differences, with strong governance organizations scoring consistently higher across all metrics. Complementing this, Figure 2 presents a heatmap displaying incident frequencies across 15 organizations sorted by governance score. It clearly shows that lower governance scores are associated with higher frequencies of unauthorized access, misconfiguration exploits, ransomware attacks, insider breaches, and phishing incidents.

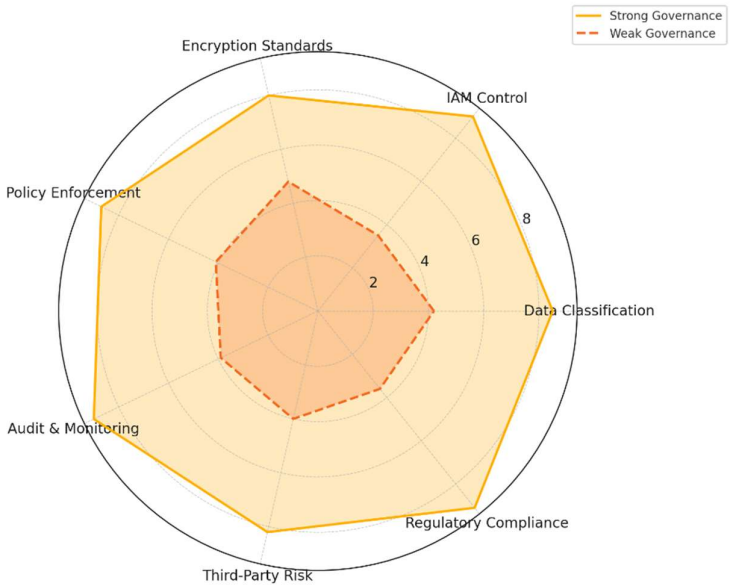

Figure 1: Radar Chart – comparative performance on governance dimensions

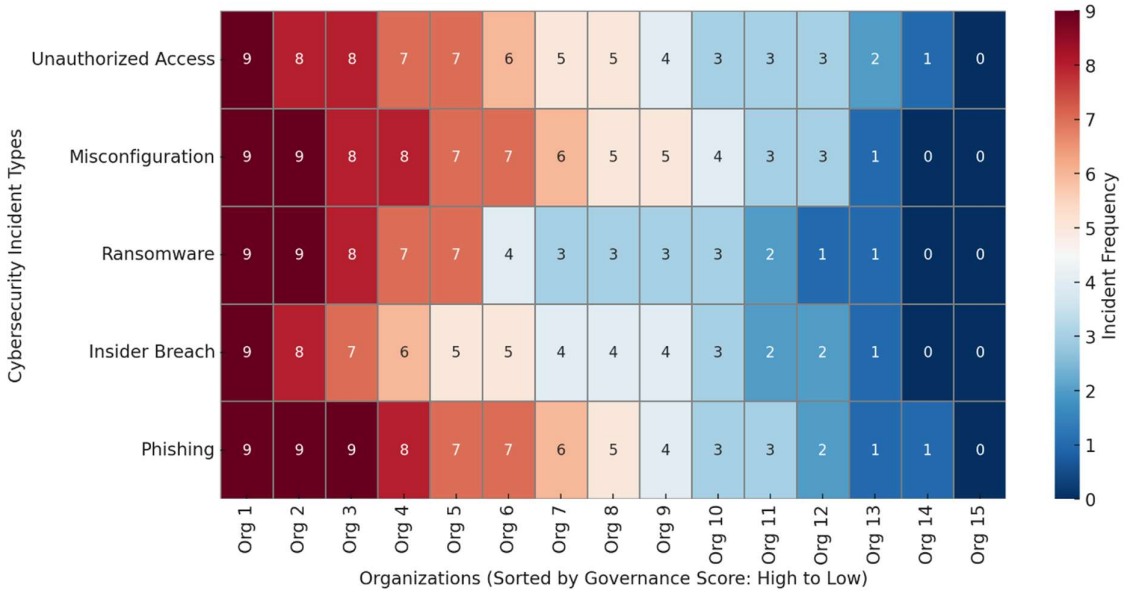

Figure 2: Heat Map – Incident Frequency vs. Governance Score

Discussion

The findings of this study underscore a compelling and statistically validated connection between weak data governance and heightened cybersecurity risk in cloud-based databases. The results provide multi-dimensional evidence-quantitative, qualitative, and visual—that poor governance

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

practices significantly increase the frequency, severity, and impact of cybersecurity incidents. This aligns with the broader cybersecurity literature emphasizing that technical defenses alone are insufficient without robust data management and policy enforcement frameworks.

Weak governance as a critical risk factor

Organizations with weak data governance consistently exhibited higher Cybersecurity Incident Scores (CIS), longer incident response times, and more frequent data breaches. As shown in Table 1, sectors such as healthcare and e-commerce where data sensitivity and transaction volumes are high were disproportionately affected when governance mechanisms were underdeveloped (Shukla et al., 2023). These organizations lacked basic controls such as data classification policies, consistent identity and access management (IAM), and encryption standards, leaving them vulnerable to misconfiguration exploits, unauthorized access, and insider threats (). The heatmap in Figure 2 vividly illustrates this pattern, with higher incident frequencies clustering among organizations with low governance scores.

Strong governance enhances cybersecurity performance

In contrast, organizations with mature data governance frameworks not only experienced fewer cybersecurity incidents but also responded more swiftly and effectively to those that did occur. As revealed in Table 3, these organizations had significantly lower CIS values and faster response times ($p < 0.001$), suggesting that governance maturity translates into operational preparedness. The radar chart in Figure 1 supports this, showing consistently higher scores across critical governance dimensions like policy enforcement, regulatory compliance, and third-party risk management (Irsheid et al., 2022). These results reflect industry best practices, where proactive governance such as regular audits, automated access controls, and cloud resource monitoring serves as a foundational layer for cybersecurity (Kathuria et al., 2019).

Governance maturity as a predictor of risk

The regression analysis in Table 4 demonstrates that governance effectiveness is not just correlated with cybersecurity outcomes but is a statistically significant predictor (. A one-point increase in the Governance Effectiveness Score (GES) leads to a measurable decrease in CIS, even after adjusting for confounding variables such as sector and cloud service provider (). This finding is vital for decision-makers as it quantitatively reinforces the value of investing in governance as a form of cyber risk mitigation. Notably, the influence of compliance status on CIS suggests that adherence to frameworks like GDPR and HIPAA may serve as indirect reinforcements of governance quality (Ahmadi, 2023).

Implications for policy and practice

These insights carry substantial implications for both practitioners and policymakers (). Organizations operating in highly regulated sectors or managing sensitive customer data must prioritize data governance not just for compliance, but as a core component of their cybersecurity strategy (Gupta et al., 2023). Cloud-specific governance tools such as cloud security posture management (CSPM) solutions, automated classification systems, and continuous compliance monitoring should be integrated into governance policies to ensure visibility and control in real time (Krämer & Schnurr, 2022). Furthermore, organizations must invest in regular training for data stewards and IT staff to ensure that governance policies are correctly interpreted and applied across the enterprise (Abioye et al., 2021).

Bridging the governance gap

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

The stark contrast between governance-strong and governance-weak organizations suggests a significant "governance gap" that must be addressed. Many smaller firms or those undergoing rapid digital transformation may lack the resources or expertise to implement governance frameworks effectively (Yadav et al., 2022). For such organizations, adopting modular governance models or using managed cloud governance services may offer scalable and cost-effective solutions. Additionally, regulatory bodies and industry consortia should provide standardized templates and toolkits for cloud governance to assist organizations in aligning with best practices (Mishra et al., 2021).

The study confirms that weak data governance is not just a procedural oversight but a critical cybersecurity vulnerability. As cloud adoption accelerates, the governance-cybersecurity nexus will become increasingly central to organizational resilience (Rana et al., 2023). This study contributes to the growing body of evidence calling for integrated, policy-driven, and technology-supported approaches to data governance in the cloud era. A shift in perspective from viewing governance as a compliance burden to recognizing it as a strategic enabler of cybersecurity is urgently needed.

Conclusion

This study concludes that weak data governance significantly exacerbates cybersecurity risks in cloud-based database environments. Through a comparative analysis of organizations across healthcare, finance, and e-commerce sectors, the research demonstrates that deficiencies in governance—such as inadequate data classification, poor access controls, and lack of compliance mechanisms—are closely linked to increased data breaches, prolonged incident response times, and higher cybersecurity incident severity. Conversely, organizations with strong governance frameworks exhibit enhanced resilience, faster recovery, and reduced exposure to both external and internal threats. The results underscore that effective data governance is not merely a regulatory requirement but a strategic necessity for cybersecurity in the cloud. Strengthening governance through clearly defined policies, automated monitoring, and compliance integration can serve as a robust line of defense in today’s complex digital ecosystem. As cloud adoption continues to expand, embedding governance maturity into the core of cybersecurity planning will be crucial for safeguarding organizational data assets and maintaining trust in digital operations.

References

Abioye, T. E., Arogundade, O. T., Misra, S., Adesemowo, K., & Damaševičius, R. (2021). Cloud-based business process security risk management: A systematic review, taxonomy, and future directions. *Computers*, *10*(12), 160.

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

Ahmadi, S. (2023). Security and privacy challenges in cloud-based data warehousing: A comprehensive review. *International Journal of Computer Science Trends and Technology (IJCST)–Volume*, *11*.

Alabi, M. (2023). Data Governance and Quality: Ensuring Data Reliability and Trustworthiness.

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and ubiquitous computing*, *23*, 839-859.

Gupta, I., Singh, A. K., Lee, C. N., & Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

directions. *IEEE Access*, *10*, 71247-71277.

Irsheid, A., Murad, A., AlNajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205-217.

Kathuria, S., Grover, A., Perego, V. M. E., Mattoo, A., & Banerjee, P. (2019). *Unleashing e-commerce for South Asian integration*. World Bank Publications.

Kouatli, I. (2014). A comparative study of the evolution of vulnerabilities in IT systems and its relation to the new concept of cloud computing. *Journal of Management History*, *20*(4), 409-433.

Krämer, J., & Schnurr, D. (2022). Big data and digital markets contestability: Theory of harm and data access remedies. *Journal of Competition Law & Economics*, *18*(2), 255-322.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), 538.

Mishra, S., Alowaidi, M. A., & Sharma, S. K. (2021). Impact of security standards and policies on the credibility of e-government. *Journal of Ambient Intelligence and Humanized Computing*, 1-12.

Naik, S. (2023). Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. *The Eastasouth Journal of Information System and Computer Science*, *1*(01), 69-87.

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management*, *26*(2), 245-266.

Rana, M. E., Yik, T. M., & Hameed, V. A. (2023, July). Cloud Computing Adoption in the Banking Sector: A Comparative Analysis of Three Major CSPs. In *2023 IEEE 6th International Conference on Big Data and Artificial Intelligence (BDAI)* (pp. 244-250). IEEE.

Shukla, S., Bisht, K., Tiwari, K., & Bashir, S. (2023). Comparative study of the global data economy. In *Data economy in the digital age* (pp. 63-86). Singapore: Springer Nature Singapore.

Yadav, S., Kalaskar, K. D., & Dhumane, P. (2022). A Comprehensive Survey of IoT-Based Cloud Computing Cyber Security. *Oriental journal of computer science and technology*, *15*(1, 2, 3), 27-52.