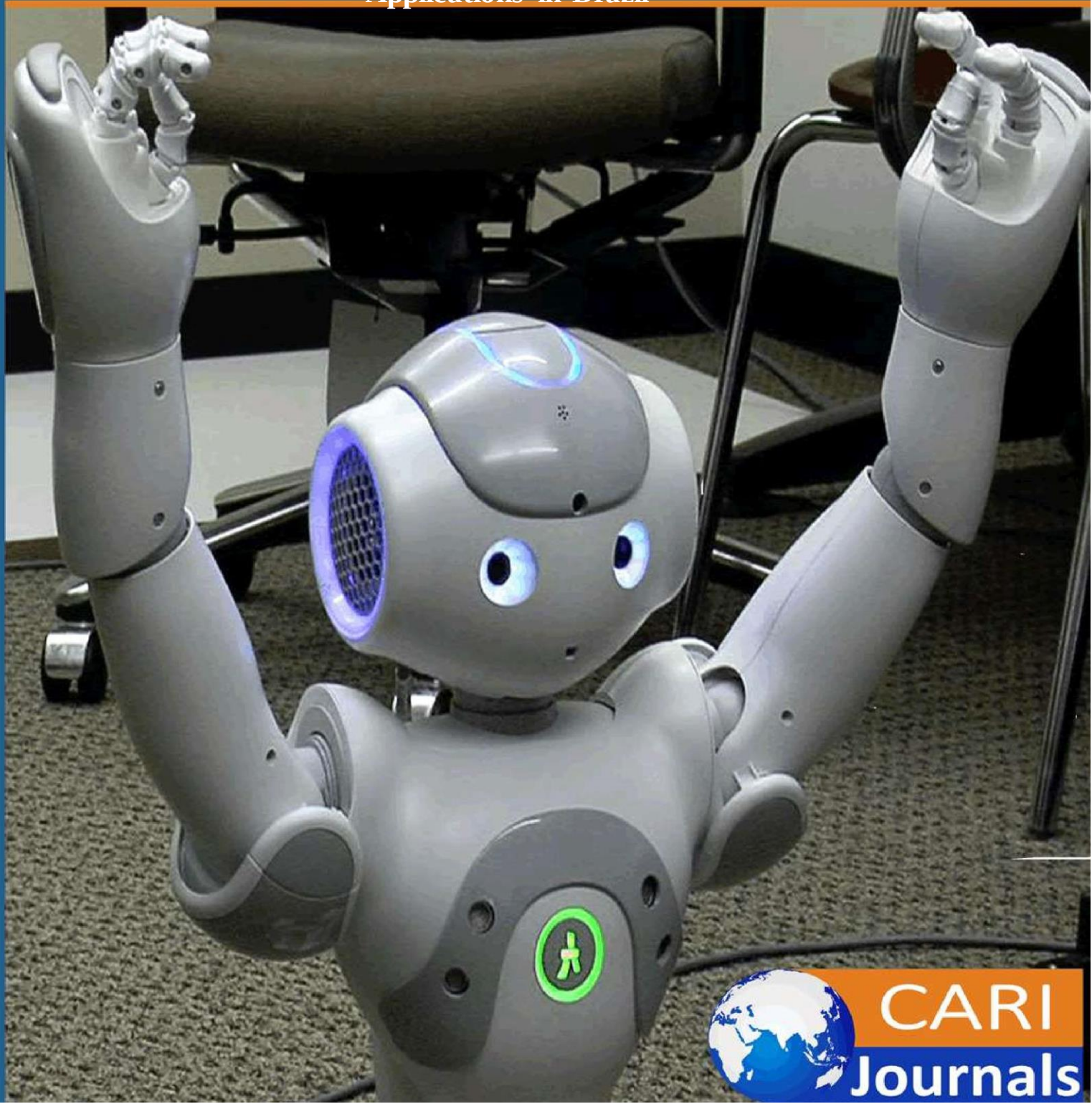
International Journal of
Computing and
Engineering
(IJCE)

# Impact of Cloud Computing on Data Security in E-Commerce Applications in Brazil



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 34 - 44, 2024
www.carijournals.org

# Impact of Cloud Computing on Data Security in E-Commerce Applications in Brazil

Alves Rocha

Universidade de Brasília (UnB)

**Abstract**

**Purpose:** The purpose of this article was to analyze impact of cloud computing on data security in e-commerce applications in Brazil.

**Methodology:** This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

**Findings:** Cloud computing has significantly impacted data security in e-commerce applications in Brazil by offering both advantages and challenges. While cloud services enhance scalability, flexibility, and cost-effectiveness, they also introduce concerns regarding data privacy, regulatory compliance, and vulnerability to cyberattacks. E-commerce businesses in Brazil face issues like data breaches and unauthorized access, which are exacerbated by insufficient local regulations and security standards. However, with proper encryption, multi-factor authentication, and adherence to global security frameworks, these risks can be mitigated.

**Unique Contribution to Theory, Practice and Policy:** Technology acceptance model (TAM), diffusion of innovations (DOI) theory, resource-based view (RBV)may be used to anchor future studies on the impact of cloud computing on data security in e-commerce applications in Brazil. From a practical standpoint, e-commerce businesses leveraging cloud computing must adopt a multi-layered security approach to protect sensitive data. Policymakers should focus on creating comprehensive cloud security standards tailored to the needs of the e-commerce sector.

**Keywords:** *Cloud Computing, Data Security, E-Commerce Applications*

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 34 - 44, 2024
www.carijournals.org

## INTRODUCTION

Data security measures in developed economies like the USA and Japan, data security is paramount, with organizations implementing robust measures to protect sensitive information. In the United States, the healthcare sector has seen a significant rise in data breaches, with 725 incidents reported in 2023 alone, exposing over 133 million records. These breaches were predominantly due to hacking and IT incidents. To combat this, organizations are increasingly adopting encryption technologies and complying with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) to safeguard data. Similarly, Japan has experienced substantial data breaches, notably the 2014 Benesse Corporation leak, which affected nearly 29 million individuals. In response, Japan amended its Act on the Protection of Personal Information in 2015 to enhance data protection and breach notification protocols. These measures aim to improve transparency and accountability in handling personal data (Thales Group, 2023; Wall Street Journal, 2023).

In developing economies, data security challenges are compounded by limited resources and infrastructure. For instance, in India, the healthcare sector has witnessed a surge in cyberattacks, with ransomware attacks increasing by 278% between 2018 and 2023. Despite these threats, many organizations struggle to implement comprehensive encryption and access control measures due to budgetary constraints. However, initiatives like the Digital India program aim to bolster cybersecurity frameworks and promote data protection awareness. In Brazil, the General Data Protection Law (LGPD), enacted in 2020, mandates data protection and breach notification, aligning with international standards. While enforcement is ongoing, the law represents a significant step towards enhancing data security in the region (Cobos & Lichtenstein, 2023).

Sub-Saharan Africa faces unique data security challenges, including limited regulatory frameworks and inadequate infrastructure. In South Africa, the Protection of Personal Information Act (POPIA) was enacted to regulate data processing activities and protect personal information. However, enforcement remains a challenge, and many organizations lack the resources to implement robust security measures. In Kenya, the enactment of the Data Protection Act in 2019 marked progress towards establishing a legal framework for data protection. Nonetheless, the country faces challenges in enforcement and capacity building to ensure compliance and enhance data security (Bouke, 2023; Lekota & Coetzee, 2022).

Cloud computing services can be broadly categorized into four types: Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud. The Public Cloud is owned and managed by third-party providers and offers services to multiple customers, often at a lower cost but with increased exposure to security breaches. Private Cloud is dedicated to a single organization, offering more control over security and compliance but at a higher cost. The Hybrid Cloud combines both private and public clouds, allowing businesses to keep sensitive data secure while taking advantage of public cloud services for less critical operations. Finally, Community Cloud is shared by multiple organizations with common concerns, offering a balance between cost and security but still vulnerable to targeted attacks due to the shared infrastructure.

Each cloud service type has distinct implications for data security. In Public Cloud environments, while encryption can protect data, the risk of data breaches is higher due to the shared nature of resources (Amazon Web Services, 2021). Private Clouds, however, are often equipped with

enhanced security measures like stricter access controls and end-to-end encryption, minimizing the risk of breaches (IBM, 2022). Hybrid Clouds enable businesses to maintain sensitive data within a private cloud while utilizing public cloud resources for scalability, which can reduce exposure but requires strong integration security protocols (Microsoft, 2023). Community Cloud offers a middle ground, allowing organizations with similar security concerns to share infrastructure while following common compliance standards, yet still facing potential vulnerabilities from shared access.

**Problem Statement**

The integration of cloud computing into e-commerce platforms has revolutionized business operations by enhancing scalability, flexibility, and cost-efficiency. However, this transition has introduced significant data security challenges. Despite the adoption of cloud services, a substantial number of businesses continue to experience data breaches; in 2023, 39% of organizations reported such incidents, with human error being the leading cause (Thales Group, 2023). Moreover, a concerning 82% of data breaches in 2023 involved data stored in the cloud, highlighting vulnerabilities in cloud environments (Wall Street Journal, 2023).

These security issues are exacerbated by factors such as inadequate encryption practices, with only 45% of sensitive cloud data being encrypted on average (Thales Group, 2023), and the complexities arising from multi-tenancy in cloud infrastructures, which can lead to data leakage between clients (Wikipedia, 2023). Additionally, the rapid adoption of cloud services without comprehensive security strategies has increased the attack surface, making e-commerce platforms more susceptible to cyber threats (Thales Group, 2023).

**Theoretical Review**

**Technology Acceptance Model (TAM)**

Developed by Fred Davis in 1989, TAM posits that perceived usefulness and perceived ease of use significantly influence users' decisions to accept and use technology. In the context of e-commerce, TAM helps explain how businesses and consumers perceive cloud computing technologies, especially concerning data security features like encryption and access controls. Understanding these perceptions is crucial for assessing the adoption and effective utilization of cloud services in e-commerce platforms. Recent studies have extended TAM to include factors such as trust and privacy concerns, highlighting their impact on technology acceptance in digital environments (Rogers, 2018).

**Diffusion of Innovations (DOI)**

Proposed by Everett Rogers in 1962, DOI theory examines how, why, and at what rate new ideas and technology spread among cultures. In e-commerce, this theory is instrumental in understanding how cloud computing innovations, particularly those enhancing data security, are adopted across different organizations. Factors such as perceived relative advantage, compatibility, complexity, trialability, and observability influence the rate of adoption. Recent research has applied DOI to explore the challenges and pathways in adopting cloud computing innovations, emphasizing the need for comprehensive frameworks that address both security and management issues (Gokhale, 2022).

**Resource-Based View (RBV)**

Originating from the work of Wernerfelt in 1984 and further developed by Barney in 1991, RBV focuses on the strategic resources and capabilities that organizations possess, which can provide competitive advantages. In the realm of e-commerce, cloud computing can be viewed as a strategic resource that enhances data security capabilities, such as secure data storage and disaster recovery solutions. By leveraging these cloud-based resources, e-commerce businesses can strengthen their data security posture, thereby gaining a competitive edge in the digital marketplace. Recent studies have explored how organizations can strategically deploy digital resources, including cloud computing, to secure competitive advantages in the digital landscape (Patel & Kumar, 2021).

**Empirical Review**

Athamakuri & Thiruveedula (2025) investigated how cloud computing influences e-commerce performance and innovation. Their research focused on surveying e-commerce firms that have integrated cloud-based solutions into their operations, assessing how cloud technology affects various aspects of their business. The study explored the enhancements that cloud computing brings to operational efficiency, customer experience, and scalability, enabling businesses to provide a more personalized shopping experience. Additionally, cloud technology allows for rapid product and service development, which has become increasingly important in the fast-paced e-commerce environment. The findings indicate that businesses can scale their operations seamlessly, improving response times and service delivery. Furthermore, they found that cloud computing fosters greater flexibility in the development and testing of new business solutions, ultimately contributing to higher customer satisfaction. The study concluded that cloud integration leads to more agile and efficient e-commerce platforms. The recommendations provided emphasized that businesses should leverage cloud services to optimize supply chains, enhance website performance, and foster innovation by integrating enhanced data analytics capabilities. By focusing on cloud-based innovations, e-commerce companies can maintain a competitive edge in the ever-evolving digital market. Cloud solutions also allow e-commerce firms to handle large volumes of data without compromising performance. Overall, Athamakuri and Thiruveedula's study highlights the transformative impact of cloud technology on e-commerce performance and the continuous innovation required to stay relevant.

Shirazi, Seddighi, & Iqbal (2017) aimed to develop a comprehensive taxonomy that captures both traditional and emerging security challenges in cloud computing. Through an extensive content analysis of the literature on cloud computing security, the researchers sought to identify both known vulnerabilities and new threats that have emerged with the widespread adoption of cloud services. The study emphasized the importance of addressing security risks such as virtualization security, trust between cloud providers and clients, and data privacy, which are particularly pertinent in e-commerce applications where sensitive customer data is involved. They also identified concerns related to legal compliance, with businesses needing to comply with regulations like GDPR and CCPA when their data is stored on cloud platforms. One of the critical findings was the growing threat of cyberattacks targeting cloud environments, particularly when it comes to multi-tenant cloud infrastructure. The study suggested that to mitigate these risks, organizations should adopt a "Privacy-by-Design" approach to security, integrating privacy measures directly into the design of cloud solutions from the outset. The researchers recommended that businesses also implement encryption at rest and during transmission, use robust identity and

access management protocols, and conduct regular security audits. Furthermore, the study underscored the need for ongoing risk assessments and real-time monitoring of cloud environments to detect and respond to potential threats quickly. This work contributed to the development of cloud security frameworks that focus on proactive security measures and compliance. By adopting these practices, e-commerce businesses can significantly reduce the likelihood of data breaches and ensure that their cloud infrastructure remains secure.

Ola & Egho-Promise (2020) conducted a case study to apply threat modeling techniques to the migration of an e-commerce platform to the public cloud. The study aimed to identify and evaluate the potential security risks during the migration process, using threat modeling as a method to uncover vulnerabilities that may not be immediately apparent. The researchers found that cloud migrations are complex and involve various risks, including unauthorized access, data breaches, and the loss of data control. By using different threat modeling techniques, such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege), they were able to pinpoint specific threats at each stage of the migration process. Their analysis showed that while cloud migration offers scalability and operational flexibility, it also increases the attack surface, exposing e-commerce platforms to cyber threats. The findings highlighted the necessity for e-commerce businesses to adopt threat modeling throughout the migration process, ensuring they identify and address security vulnerabilities before they escalate. The study recommended that e-commerce platforms engage in regular security assessments and implement advanced security tools like intrusion detection systems and multi-factor authentication during the migration process. Additionally, it stressed the importance of educating employees on security risks and best practices for cloud usage. The researchers concluded that effective use of threat modeling not only minimizes the risks associated with cloud migration but also strengthens overall cloud security for e-commerce businesses.

Roy (2014) explored the role of cloud computing in e-commerce, particularly focusing on its impact on data security and privacy. The study aimed to examine the benefits of cloud computing, including scalability and cost-effectiveness, while addressing the associated security risks that e-commerce businesses face when adopting cloud services. Through a detailed literature review, Roy identified that while cloud computing offers significant advantages, such as the ability to handle large data volumes and provide on-demand services, it also introduces challenges related to data protection. The study found that data security in the cloud is a major concern for e-commerce businesses, particularly in terms of unauthorized access, data breaches, and loss of control over sensitive customer information. Roy emphasized the importance of adopting strong security frameworks that ensure the confidentiality, integrity, and availability of data stored in the cloud. The study recommended that businesses implement robust encryption protocols, utilize multi-factor authentication, and continuously monitor cloud environments to detect and prevent potential security incidents. Additionally, businesses were urged to ensure compliance with data protection laws such as GDPR, which governs the collection and processing of personal data. The findings underscored the need for a balance between the benefits of cloud computing and the necessary security measures to protect customer data. The research concluded that e-commerce companies must prioritize data security and adopt a comprehensive approach to protect their cloud-based systems.

Nestify (2023) explored how cloud computing enhances the performance and security of e-commerce platforms. This case study involved analyzing e-commerce companies that have integrated cloud services into their platforms, examining how cloud computing impacts their operational efficiency and data security. The study revealed that cloud computing provides e-commerce businesses with a significant advantage by improving website performance through faster content delivery and more reliable uptime. The use of content delivery networks (CDNs) and caching mechanisms allows for faster page load times, which enhances the overall user experience. Furthermore, cloud-based solutions provide advanced security features, including data encryption, secure data storage, and proactive threat detection systems. These security measures help e-commerce businesses protect sensitive customer data from cyber threats and ensure compliance with privacy regulations. The findings suggest that e-commerce companies can reduce their security risks by adopting cloud solutions that offer built-in security features and compliance tools. The study recommends that businesses continue to leverage cloud services to improve both performance and security, as they provide a scalable and secure infrastructure for growing e-commerce platforms. In addition, the research suggests that businesses should invest in security training for their employees to enhance awareness and improve their overall security posture.

Savithi & Suttidee (2024) examined the influence of information reliability and system performance on the adoption of cloud computing in e-commerce businesses. Through a literature review and the development of a conceptual research model, the researchers found that information reliability and system performance were critical factors that e-commerce businesses consider when adopting cloud services. The study revealed that businesses are more likely to adopt cloud computing if they perceive the cloud provider's system to be reliable and capable of handling large volumes of transactions efficiently. Additionally, data privacy concerns play a significant role in the decision-making process. The researchers emphasized that businesses must ensure robust data protection measures are in place, such as encryption and secure access controls, to mitigate privacy risks. The study recommended that e-commerce businesses focus on ensuring information reliability and system performance to foster customer trust and encourage wider adoption of cloud computing solutions. E-commerce platforms that ensure these factors are met can enhance user satisfaction, which in turn drives greater adoption of cloud technologies. Furthermore, the researchers suggested that cloud providers should continue to improve system performance and address security concerns to remain competitive in the e-commerce sector.

Aksakal (2023) aimed at protecting e-commerce businesses from cyberattacks while utilizing cloud computing. Through a systematic literature review and case study analysis, Aksakal identified key vulnerabilities in cloud environments that could be exploited by cybercriminals, such as weak authentication mechanisms, inadequate encryption practices, and poor data management policies. The study developed a cybersecurity model that integrates both offensive and defensive strategies, focusing on proactive threat detection, real-time monitoring, and quick response mechanisms to mitigate security breaches. The researcher highlighted the importance of developing a security-first culture within organizations and ensuring that cybersecurity measures are implemented at every stage of cloud deployment. The study recommends that e-commerce businesses adopt a holistic approach to cloud security by implementing the proposed cybersecurity model, which includes both prevention and response strategies to combat emerging threats. This model can help businesses strengthen their cloud security posture, protect sensitive customer data, and avoid costly data breaches. E-commerce companies are encouraged to work closely with their

cloud providers to ensure that security measures are continuously updated and aligned with the latest cybersecurity trends.

## METHODOLOGY

This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low-cost advantage as compared to field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

## FINDINGS

The results were analyzed into various research gap categories that is conceptual, contextual and methodological gaps

**Conceptual Gaps:** While several studies examine cloud computing's impact on data security in e-commerce applications, there is a lack of comprehensive frameworks that directly integrate cloud security with performance and scalability measures. For example, Athamakuri & Thiruveedula (2025) explored how cloud technology enhances operational efficiency and scalability, but did not address the specific conceptual frameworks that link these advantages to security risks. The existing research largely focuses on isolated security features such as encryption and data privacy, but fails to provide a unified, conceptual model that merges performance optimization with secure cloud adoption. Further conceptual development is needed to create models that can effectively integrate the benefits of cloud technology with the emerging risks, offering businesses a holistic view of both security and performance.

**Contextual Gaps:** Many studies, including Shirazi, Seddighi, & Iqbal (2017) and Ola & Egho-Promise (2020), highlight the importance of cloud security frameworks but focus on generalized approaches that may not fully account for the specific needs of e-commerce applications. For instance, Shirazi (2017) addressed broad cloud security challenges like data privacy and legal compliance, but did not explore how these issues uniquely affect the fast-paced, customer-centric environment of e-commerce. Additionally, while Roy (2014) emphasized data security risks like unauthorized access and data breaches, the context of how businesses adopt cloud solutions specifically for e-commerce growth and customer interaction was not fully explored. There is a need for more context-specific research that examines how cloud security can be optimized for e-commerce business models, which rely heavily on customer data, personalization, and scalability.

**Geographical Gaps:** Geographical considerations also present a gap in the literature. Most of the studies, including Savithi & Suttidee (2024) and Aksakal (2023), are general and do not account for regional or geographical differences in how cloud computing and its associated security challenges are approached. For example, Nestify (2023) and Shirazi (2017) analyze the technical aspects of cloud security, but they do not provide region-specific insights on how e-commerce businesses in different countries (especially those in emerging economies) address these challenges. In regions like Sub-Saharan Africa or parts of Asia, where cloud computing adoption might be slower or infrastructure may differ, the same security risks and solutions may not apply. More research is needed to address geographical differences in the adoption of cloud services and the unique data security challenges faced by e-commerce businesses in specific regions.

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 34 - 44, 2024
www.carijournals.org

## CONCLUSION AND RECOMMENDATIONS

### Conclusions

The integration of cloud computing into e-commerce applications has revolutionized the industry by offering scalability, cost-efficiency, and flexibility. However, it has also introduced significant data security challenges that require careful attention. Cloud-based e-commerce platforms are particularly vulnerable to risks such as data breaches, unauthorized access, and loss of control over sensitive consumer data. As businesses continue to migrate to the cloud, ensuring robust data security measures becomes paramount to maintaining consumer trust and regulatory compliance. The key to addressing these challenges lies in a multi-layered security approach that combines encryption, tokenization, and multi-factor authentication with strong due diligence when selecting cloud providers. Additionally, the evolving regulatory landscape requires businesses to stay vigilant in ensuring compliance with data protection laws such as GDPR and CCPA, particularly as data is often stored and processed across multiple jurisdictions.

The development of new theoretical models, practical security measures, and global policy frameworks will play a critical role in mitigating the risks associated with cloud computing in e-commerce. By investing in advanced security technologies, encouraging transparency in cloud contracts, and promoting international cooperation on data protection, stakeholders can create a safer and more secure digital environment for both businesses and consumers.

### Recommendations

#### Theory

The intersection of cloud computing and e-commerce presents new security challenges that existing data security models may not fully address. Researchers should explore the development of new theories that account for the specific vulnerabilities introduced by the cloud environment, such as multi-tenancy, data migration, and limited control over infrastructure. Existing security frameworks, like the CIA triad (Confidentiality, Integrity, Availability), should be expanded to incorporate new dimensions of cloud security risks in e-commerce applications. Additionally, integrating blockchain technology with cloud computing security can provide valuable insights into how decentralized and transparent systems could enhance data protection and fraud prevention for e-commerce platforms. Theoretical contributions in these areas will help deepen our understanding of the risks and solutions surrounding data security in cloud-based e-commerce systems.

#### Practice

From a practical standpoint, e-commerce businesses leveraging cloud computing must adopt a multi-layered security approach to protect sensitive data. This includes the implementation of encryption, tokenization, and multi-factor authentication across all touchpoints of the cloud infrastructure. These measures ensure that even if one layer is compromised, others will still safeguard the data. Additionally, e-commerce companies should ensure compliance with data protection regulations like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). By choosing cloud providers that offer robust data localization and protection mechanisms, businesses can mitigate the risk of non-compliance and ensure that data is managed within secure legal boundaries. Rigorous due diligence in selecting cloud

providers, coupled with regular security audits, is also essential to ensure ongoing security and compliance. Training internal teams on cloud security best practices will further reduce the risk of human error, a common vulnerability in cloud environments.

**Policy**

Policymakers should focus on creating comprehensive cloud security standards tailored to the needs of the e-commerce sector. These standards should include mandatory encryption practices, breach notification protocols, and the establishment of standardized risk assessments for cloud service providers. This will help streamline security practices across the e-commerce industry and provide a consistent framework for protecting customer data. In addition, governments should encourage transparency in cloud service contracts, ensuring that agreements clearly outline data ownership, breach responsibilities, and retention policies. Such measures will help e-commerce businesses navigate the complex relationships with cloud providers and reduce security uncertainties. Public policies should also incentivize e-commerce businesses to invest in advanced cloud security technologies, offering tax breaks or grants to small and medium enterprises that adopt robust security measures. Furthermore, policymakers need to establish international agreements for cross-border data flows, ensuring that data protection laws are upheld globally, which will reduce security risks associated with storing and transferring data across multiple jurisdictions.

**REFERENCES**

Aksakal, C. (2023). Security model for cloud computing: Case report of e-commerce. Journal of Computer Networks and Communications, 2023, 1–10. https://doi.org/10.1155/2023/126892

Amazon Web Services. (2021). AWS Cloud security best practices. Retrieved from https://aws.amazon.com/security/

Athamakuri, S. S. K., & Thiruveedula, J. (2025). The impact of cloud computing on e-commerce performance and innovation: An empirical study. International Journal of Research in Modern Engineering & Emerging Technology, 13(3), 328–350. https://doi.org/10.63345/ijrmeet.org.v13.i3.21

Bouke, M. A., Abdullah, A., ALshatebi, S. H., El Atigh, H., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions. Journal of Cybersecurity and Privacy, 3(1), 1-20. https://doi.org/10.3390/jcp3010001

Cobos, E. V., & Lichtenstein, S. (2023). A review of the economic costs of cyber incidents. World Bank Policy Research Working Paper No. 10234. https://doi.org/10.1596/1813-9450-10234

CPL Thales Group. (2023). 2023 Cloud Security, Cyberattacks, and Data Breaches Press Release. Retrieved from https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release

IBM. (2022). What is private cloud computing?. Retrieved from https://www.ibm.com/cloud/learn/private-cloud

Ishii, K., & Komukai, T. (2016). Data breach notification laws in Japan: A cultural perspective. Asian Journal of Comparative Law, 11(2), 123-145. https://doi.org/10.1017/asjcl.2016.9

Lekota, F., & Coetzee, M. (2022). Cybersecurity incident response for the Sub-Saharan African aviation industry. Journal of Cybersecurity in Africa, 5(1), 33-47. https://doi.org/10.1016/j.jcsa.2022.04.003

Microsoft. (2023). Hybrid cloud security for enterprises. Retrieved from https://azure.microsoft.com/en-us/overview/what-is-hybrid-cloud/

Nestify. (2023). Cloud computing for e-commerce: Boosting performance and security. Retrieved from https://nestify.io/blog/cloud-computing-for-ecommerce/

Nyoni, P. (2024). Privacy perceptions on personal data and data breaches in Sub-Saharan Africa. African Journal of Information Systems, 16(1), 1-15. https://doi.org/10.2139/ssrn.3667612

Ola, B., & Egho-Promise, I. (2020). Cybersecurity threat modelling: A case study of an e-commerce platform migration to the public cloud. European Journal of Electrical Engineering and Computer Science, 4(4), 237–245. https://doi.org/10.24018/ejece.2020.4.4.237

Roy, S. (2014). Data security and influence of cloud computing in electronic commerce industry. International Journal of Computer Applications, 97(1), 1–5. https://doi.org/10.5120/17106-3653

Savithi, C., & Suttidee, A. (2024). The impact of information reliability and cloud computing on e-commerce. Journal of Computer Science, 20(2), 198–206. https://doi.org/10.3844/jcssp.2024.198.206

Seh, A. H. (2020). Healthcare data breaches: Insights and implications. Journal of Healthcare Information Management, 34(2), 45-52. https://doi.org/10.1016/j.jhim.2020.02.003

Shirazi, F., Seddighi, A., & Iqbal, A. (2017). Cloud computing security and privacy: An empirical study. Journal of Cloud Computing: Advances, Systems and Applications, 6(1), 1–14. https://doi.org/10.1186/s13677-017-0097-1

Thales Group. (2023). 2023 Cloud Security, Cyberattacks, and Data Breaches Press Release. Retrieved from https://cpl.thalesgroup.com/about-us/newsroom/2023-cloud-security-cyberattacks-data-breaches-press-release

Wall Street Journal. (2023). Why Are Cybersecurity Data Breaches Still Rising? Retrieved from https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c

Wikipedia. (2023). Cloud Computing Security. Retrieved from https://en.wikipedia.org/wiki/Cloud_computing_security

World Bank. (2023). Regulating digital data in Africa. World Bank Report. https://openknowledge.worldbank.org/bitstreams/62e27761-1da1-467f-99a2-a6a1a3cf3b54/download