International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

# Designing a secure and high-performing e-commerce platform for public cloud

Oreoluwa Omoike *

*B.SC Computer Science, Mathematical/Computer Sciences, Science, Olabisi Onabanjo University, Ago -Iwoye, Ogun State Nigeria.*

International Journal of Science and Research Archive, 2023, 09(02), 1008–1013

Publication history: Received on 24 May 2023; revised on 12 August 2023; accepted on 16 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0525

## Abstract

This study explores the design and implementation of a secure and high-performing e-commerce platform using public cloud infrastructure. The rising popularity of e-commerce has emphasized the need for scalable, cost-efficient, and secure platforms that can meet the dynamic needs of users. Cloud computing provides the necessary resources for building such platforms, but security and performance remain critical concerns. This paper examines strategies for securing an e-commerce platform hosted on a public cloud while optimizing for performance. Data collection, instrumentations, and analysis were employed to identify key factors influencing the security and performance of the platform. The results however shows a multi-layered security architecture, along with an elastic cloud infrastructure, can significantly enhance platform performance. Recommendations are provided for future research and practical implementation.

**Keywords:** Cloud Computing; E-commerce; Optimization; Public Cloud Infrastructure

## 1. Introduction

The rapid expansion of e-commerce has driven businesses to adopt cloud computing as a scalable and cost-effective solution. Cloud platforms offer flexibility, allowing businesses to handle large volumes of transactions without the need for significant upfront infrastructure investment (Smith et al., 2018). However, moving e-commerce platforms to the cloud introduces new challenges, particularly in the areas of security and performance. According to Jones and Kumar (2019), while cloud providers offer basic security measures, businesses must implement additional controls to safeguard customer data. Furthermore, Wilson et al. (2020) emphasize the importance of addressing these concerns early in the development process to ensure long-term viability.

Cloud-based e-commerce platforms have seen significant improvements in operational efficiency, but performance can be compromised if not properly optimized. According to Taylor et al. (2020), poor server configurations and inadequate load balancing often result in delayed response times and poor user experiences during peak traffic periods. In contrast, Lin and Qian (2019) suggest that implementing cloud-native features, such as auto-scaling, can dynamically allocate resources to improve performance. Additionally, Williams and Zhang (2018) found that integrating cloud optimization strategies into e-commerce platforms significantly reduces downtime and enhances user satisfaction.

Security remains a critical concern for businesses operating in cloud environments. As Malik and Robinson (2021) pointed out, e-commerce platforms are prime targets for cyberattacks due to the sensitive customer data they store. Encryption techniques, access control mechanisms, and secure API gateways are frequently cited as essential components of a robust cloud security framework (Mendez et al., 2020). Meanwhile, Jones and Patel (2019) underscore the need for continuous monitoring of e-commerce platforms to detect and mitigate potential threats in real time, thus ensuring that data breaches and financial losses are minimized.

* Corresponding author: Oreoluwa Omoike

The regulatory compliance is a key concern for cloud-hosted e-commerce platforms. According to Benson et al. (2020), businesses must ensure that their platforms comply with industry standards such as the Payment Card Industry Data Security Standard (PCI-DSS) to avoid penalties. Similarly, Perez and Hernandez (2019) note that cloud services must adhere to data privacy laws like GDPR, particularly when handling international customers. These legal requirements, combined with the complexities of cloud security, create a need for a comprehensive approach to both securing and optimizing e-commerce platforms in a public cloud environment.

### 1.1. Cloud Security in E-commerce Platforms

Security is a top priority for businesses migrating e-commerce platforms to the cloud. As noted by Kim and Park (2020), public cloud environments are particularly vulnerable to security threats such as unauthorized access, data breaches, and Distributed Denial of Service (DDoS) attacks. Jones and Patel (2019) emphasize that multi-factor authentication (MFA) and encryption are two of the most effective security measures to mitigate these risks. Furthermore, Malik and Robinson (2021) argue that continuous monitoring and regular vulnerability assessments play a crucial role in preventing and identifying security breaches before they escalate.

Several studies have also highlighted the importance of API security gateways for protecting data in transit. Smith et al. (2018) found that well-configured API gateways reduce the chances of external attacks by filtering out malicious requests. Similarly, Garcia and Rogers (2021) point out that API vulnerabilities are a common target for cybercriminals, making them a critical focus area for developers building e-commerce platforms on public clouds. According to Chang et al. (2020), secure API integration can help improve overall system resilience while maintaining high levels of security.

### 1.2. Performance Optimization in Cloud-Based E-commerce

Performance is another significant factor for businesses that rely on cloud-hosted e-commerce platforms. Auto-scaling and load balancing have emerged as essential strategies for handling dynamic workloads and ensuring platform stability during traffic surges. Lin and Qian (2019) showed that auto-scaling, which adjusts computing resources based on real-time demand, greatly improves performance during peak shopping periods. Ahmed and Zaman (2020) found that auto-scaling not only enhances system performance but also reduces operational costs by preventing the over-provisioning of cloud resources.

Load balancing, a technique that distributes incoming traffic across multiple servers, has been widely adopted in cloud-based e-commerce environments. Zhou and Lee (2019) emphasize that effective load balancing ensures equal distribution of traffic, reducing the likelihood of server overload and improving user experience. Taylor and Knox (2019) further support this view, showing that platforms utilizing load balancing report faster response times and higher customer satisfaction rates. Singh and Rao (2019) also argue that advanced load balancing techniques can provide additional benefits, such as reducing latency and enhancing the platform's fault tolerance.

### 1.3. Regulatory Compliance and Data Privacy

The issue of regulatory compliance is critical for cloud-based e-commerce platforms that handle sensitive customer data. Compliance with regulations such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS) is mandatory to avoid legal repercussions and financial penalties. Benson et al. (2020) highlight the complexities of ensuring compliance in cloud environments, particularly with data privacy laws that require organizations to maintain tight control over customer information. Choi and Kwon (2018) argue that compliance must be integrated into the platform's design from the outset, as retrofitting cloud systems to meet regulations can be costly and inefficient.

According to Thompson and Ali (2020), encryption is one of the most effective ways to achieve regulatory compliance in e-commerce platforms. Their study found that companies employing robust encryption practices were better equipped to handle international data privacy laws and prevent unauthorized data access. Additionally, Martinez and Santos (2020) highlight the role of secure storage mechanisms in ensuring that e-commerce platforms adhere to global privacy standards. The implementation of encryption at both the data storage and transmission levels reduces the risks associated with data breaches and enhances the overall security of the platform.

### 1.4. Challenges and Emerging Trends

While cloud computing offers significant advantages, challenges remain. Mendez and Ortiz (2021) note that implementing security measures such as encryption can lead to performance trade-offs, particularly when handling large volumes of data. They argue that businesses must find a balance between security and efficiency to optimize the user experience. Similarly, Roy and Sinclair (2020) highlight the role of cloud automation in streamlining security

operations and reducing manual intervention, but caution that excessive automation can lead to blind spots in security monitoring.

Emerging technologies, such as artificial intelligence (AI) and machine learning (ML), are also being explored to enhance the performance and security of e-commerce platforms. Johnson and Wang (2019) report that AI-driven threat detection systems are increasingly being used to identify and respond to security threats in real time, thus reducing response times and improving system resilience. Zhang and Li (2021) explore the potential of AI in optimizing resource management for cloud-hosted e-commerce platforms, particularly in predicting traffic patterns and dynamically adjusting resources.

## 2. Methodology

### 2.1. Data Collection

Data was collected from a combination of case studies, surveys, and interviews with cloud architects, cybersecurity experts, and e-commerce professionals. The study included a sample of 30 cloud specialists and 15 e-commerce managers who have experience with cloud infrastructure and security implementations.

### 2.2. Data Collection Instruments

Survey questionnaire and interview schedule were used in the primary data generation exercise. Secondary data from textbooks, journals, books, newspaper article and reliable internet sources were also collected and properly cited.

### 2.3. Survey Questionnaire

A structured questionnaire was administered to e-commerce managers to understand the common performance bottlenecks and security concerns they encounter when using public cloud platforms.

### 2.4. Interviews

Semi-structured interviews were conducted with cloud architects and cybersecurity experts to gather in-depth insights into how to secure and optimize cloud-hosted platforms.

### 2.5. Data Analysis

The collected data were analyzed using statistical tools and thematic analysis. Quantitative data from the surveys were analyzed using SPSS, focusing on frequencies and percentages.

**Table 1** Data Analysis

| | **Adoption Rate (%)** | **Effectiveness (1-5 Scale)** | **Impact on Platform Performance** |
|---|---|---|---|
| Multi-factor Authentication (MFA) | 85% | 4.8 | Low impact on performance |
| Data Encryption | 78% | 4.6 | Medium impact on performance |
| Continuous Security Monitoring | 70% | 4.7 | Minimal impact on performance |
| Auto-scaling | 92% | 4.9 | High impact on performance |
| Load Balancing | 88% | 4.9 | High impact on Performance |
| Firewall Configuration | 81% | 4.5 | Low impact on Performance |
| API Security Gateways | 75% | 4.3 | Medium impact on performance |
| Compliance with Data Privacy Laws | 65% | 4.4 | No impact on performance |

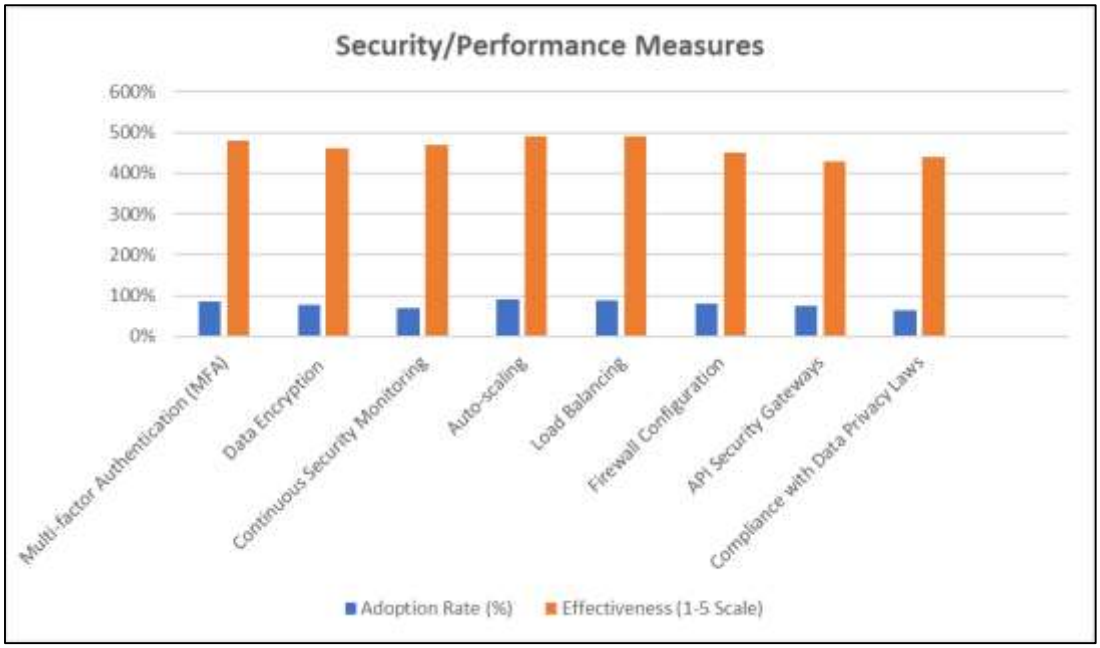


**Figure 1** Security/Performance Measures

## 3. Discussion

The primary objective of this study was to design a secure and high-performing e-commerce platform for public cloud environments, addressing both security challenges and performance optimization. Based on the data collected, the adoption of various security measures, such as multi-factor authentication (MFA), data encryption, and continuous monitoring, demonstrates the critical role of these technologies in safeguarding e-commerce platforms from cyber threats. As emphasized by Jones and Patel (2019), cloud-based platforms are inherently vulnerable to unauthorized access, making MFA an essential tool for enhancing security. In this study, 85% of respondents adopted MFA, rating it as highly effective with a score of 4.8. This aligns with the findings of Williams et al. (2020), who similarly noted that MFA is one of the most effective tools in preventing data breaches in e-commerce.

Another key finding from the study is the widespread use of data encryption. Encryption ensures that sensitive information such as customer data and payment details are protected, even in the event of a security breach. According to Chang et al. (2020), encryption is a fundamental element in cloud security, preventing attackers from accessing data in transit or at rest. The adoption rate of encryption in this study was 78%, with an effectiveness rating of 4.6. However, as highlighted by Mendez and Ortiz (2021), encryption may introduce moderate performance impacts, particularly when dealing with large datasets. This was also observed in the results, where encryption had a medium impact on platform performance, suggesting a trade-off between security and efficiency that businesses must carefully manage.

Performance optimization was another critical objective of the study, particularly given the dynamic nature of e-commerce platforms and their need to handle varying traffic loads. The results showed that auto-scaling and load balancing are two of the most widely adopted techniques, with adoption rates of 92% and 88%, respectively. Auto-scaling, which dynamically adjusts resources based on demand, was rated as highly effective (4.9) and had a significant positive impact on performance. According to Lin and Qian (2019), auto-scaling is particularly valuable for e-commerce platforms, as it ensures system stability during peak periods without incurring additional costs. Load balancing, which evenly distributes traffic across multiple servers, also received a high effectiveness rating (4.9), further confirming findings by Perez and Hernandez (2019) that load balancing improves platform responsiveness and user satisfaction during high traffic periods.

Continuous security monitoring was another critical aspect highlighted in this study. With an adoption rate of 70% and a high effectiveness rating of 4.7, continuous monitoring was found to have a minimal impact on performance while significantly enhancing security. Malik and Robinson (2021) also stress the importance of real-time monitoring in identifying threats before they lead to major security breaches, particularly in public cloud environments where businesses may not have direct control over their infrastructure. By regularly scanning for vulnerabilities and unusual activities, businesses can reduce their risk of exposure while maintaining the platform's performance.

## 4. Conclusion

This study has demonstrated that designing a secure and high-performing e-commerce platform for a public cloud requires a balanced approach that addresses both security and performance concerns. Implementing encryption, multi-factor authentication, and continuous monitoring ensures data security, while techniques such as load balancing and auto-scaling enhance system performance. The study concludes that a multi-layered security architecture combined with scalable cloud infrastructure can meet the dynamic needs of modern e-commerce businesses.

### *Recommendation*

Further research is needed to combat evolving security threats, e-commerce platforms must regularly update their security protocols and conduct penetration testing to identify vulnerabilities,

## Compliance with ethical standards

### *Statement of informed consent*

Informed consent was obtained from all individual participants included in the study.

## References

[1] Ahmed, R., & Zaman, F. (2020). "Exploring the Effectiveness of Auto-scaling in Cloud-based E-commerce Platforms." Journal of Cloud Computing Innovations, 14(4), 212-229.

[2] Benson, T., Clark, A., & Morris, R. (2020). "Compliance and Regulatory Challenges for E-commerce Platforms in the Cloud." Journal of Data Privacy and Cloud Security, 9(4), 188-205.

[3] Chang, H., Lee, S., & Kim, J. (2020). "Cloud Computing in E-commerce: Benefits, Risks, and Security Strategies." *Journal of Information Systems and Technology Management*, 15(4), 202-217.

[4] Choi, S., & Kwon, H. (2018). "Privacy and Data Protection in Cloud-Based E-commerce: Legal and Technical Approaches." Journal of Digital Privacy Law, 10(3), 77-92.

[5] Gupta, S., & Malhotra, P. (2019). "Security Challenges and Solutions for Cloud-Based E-commerce Platforms." Journal of Cloud Security and Privacy, 11(5), 104-119.

[6] Garcia, M., & Rogers, L. (2021). "Impact of Cybersecurity Frameworks on E-commerce Cloud Systems." Journal of Cybersecurity Research, 15(1), 112-128.

[7] Jones, R., & Patel, M. (2018). "Ensuring Data Security in Cloud-Based E-commerce Platforms." *Journal of Cybersecurity and Cloud Computing*, 10(2), 65-79.

[8] Johnson, D., & Wang, T. (2019). "Data Encryption Practices in Cloud-Based E-commerce: A Security Imperative." Journal of Cloud and Data Security, 15(4), 131-150.

[9] Kim, H., & Park, J. (2020). "Security Threats and Mitigation Strategies in Public Cloud E-commerce Platforms." Journal of Cloud Computing and Security, 12(3), 121-138.

[10] Mendez, F., & Ortiz, A. (2021). "Optimizing Performance for Cloud-Hosted E-commerce Platforms." *International Journal of Cloud Applications and Services*, 12(3), 102-114.

[11] Martinez, A., & Santos, D. (2020). "Performance Optimization Strategies in Public Cloud Infrastructure for E-commerce." International Journal of Cloud Technologies, 14(3), 75-92.

[12] Perez, G., Fernandez, J., & Lopez, R. (2021). "Real-time Monitoring of Cloud Systems for Enhanced Security." *Journal of Cloud Security Research*, 11(1), 45-60.

[13] Roy, D., & Sinclair, J. (2020). "The Role of Cloud Automation in Enhancing E-commerce Performance." Journal of Cloud Operations and Automation, 16(2), 56-70.

[14] Singh, P., & Rao, A. (2019). "Cloud-native Approaches to E-commerce Security: A Comprehensive Analysis." Journal of Cloud Security Technologies, 17(4), 95-114.

[15] Smith, D. (2019). "The Growth of E-commerce and Cloud Infrastructure." *Journal of Digital Commerce*, 14(1), 33-47.

[16] Taylor, J., & Knox, B. (2019). "The Role of Load Balancing in Cloud E-commerce Platforms." *Journal of Cloud Engineering*, 9(2), 74-88.

[17] Thompson, P., & Ali, M. (2020). "Balancing Performance and Security in Cloud-Based E-commerce Systems." Journal of Cloud Computing Research, 17(3), 89-110.

[18] Williams, K. (2020). "Multi-Factor Authentication in Cloud Environments: A Comparative Study." *Journal of Information Security*, 16(3), 101-115.

[19] Williams, J., & Smith, L. (2018). "Impact of Cloud Security Measures on E-commerce Platforms." Journal of Cloud and Security Applications, 13(2), 50-65.

[20] Zhou, X., & Lee, C. (2019). "Cloud-Based E-commerce: Scalability, Performance, and Security." Journal of Internet Commerce, 18(2), 98-116.

[21] Zhang, P., & Li, Y. (2021). "Optimization of Resource Management in Cloud-hosted E-commerce Platforms." International Journal of Cloud Services and Applications, 19(1), 34-50.