

COMPARATIVE STUDY OF PRIVACY-PRESERVING MEASURES IN NIGERIAN E-COMMERCE PLATFORMS

Esther Abeson Nasara* and Timothy Moses

Department of Computer Science, Faculty of Computing, Federal University of Lafia,
Nasarawa State.

*Corresponding Author: esthersam460@gmail.com

<https://doi.org/10.62050/faic2024.bop24.012>

ABSTRACT

Most Nigerian e-commerce today are faced with numerous challenges, primarily due to the pressure that exist between providing e-commerce services and protecting users personalized information. Users' details provided on these platforms are most times shared with third-party advertisers and analytics companies without users' consent. Hackers and internet fraudsters take advantage of the weakness of these platforms to obtain account details of users. An assessment of privacy-preserving strategies in Nigerian e-commerce platforms is therefore crucial in the present digital era, when online transactions and data interchange have become indispensable to the corporate environment. Because of the increased attention that privacy problems in e-commerce platforms have received, users of these platforms need to be more aware of how their personal information is treated. This article investigates privacy-preserving methods used by popular e-commerce platforms in Nigeria. The goal of the study is to present a thorough assessment of the level of privacy protection in most commonly used Nigerian e-commerce platforms. The study's recommendations are intended to direct customers, e-commerce companies, and policymakers toward a safer and more secure online buying environment in Nigeria.

Keywords: Privacy-preserving measures, e-commerce platforms, Nigerian e-commerce, online transaction, online shopping.

1.0 Introduction

The term "privacy-preserving measures" describes methods, guidelines, and tools used to protect people's private information and uphold their right to privacy in a variety of settings, especially those that use technology (Agnieszka *et. al.*, 2022). These safeguards are intended to maintain people's ownership over their personal information while guarding sensitive data from unauthorized access, disclosure, or abuse.

Online business includes the buying and selling of goods and services as well as activities involving the exchange of money and data. Secure online transactions are ensured by the e-commerce security regulation. It is made up of laws that safeguard those who sell and buy goods and services online. Any activity that could reveal client information to uninvited parties are prohibited in order to protect privacy. Only the online retailer of the customer's choice should have access to their data or account information. While e-commerce platforms have made transactions easier, scammers have gotten more active on how to obtain details of



customers who utilize these platforms. Current scholarly study suggests that the e-commerce sector is extremely susceptible to cybercrime assaults (Ghosal and Balaji, 2022).

Every electronic commerce business owner who interacts with, saves, or requests any data that may be sensitive if lost worries about security. Any company that wants to outperform its competitors has to have a thorough security strategy in consultation with partners, suppliers, and distributors that provide safe environments for operations that centered on internet commerce. Many consumers attribute their refusal to trade online to a lack of confidence or worry over the security of their personal information. Customers run the risk of giving the vendor access to sensitive personal information when they transact online. Dijesh *et. al.* (2020) assert that preserving and enhancing consumer trust is crucial to the ongoing expansion of internet commerce.

As more and more businesses shift their activities online, the need to secure our personal information online must also grow. There is a need therefore to be curious about the measures taken by well-known Nigerian e-commerce sites to safeguard customers' personal data, which includes names and the items they buy. E-commerce platforms allow Nigerian consumers to purchase items online anytime they want, which transfers a lot of data over the internet. Several forms of data are collected from users when they buy or sell things online. These include credit card numbers, personal profiles, job specifics, and, most recently, the user's state of health and fitness. Akinola and Asaolu (2023) assert that the internet presents a multitude of security dangers due to its function as a worldwide network that connects billions of devices and users. Credit card fraud and account information compromise are the two most significant security threats that are known to affect e-commerce (Shyaa and Al-Zubaidie, 2023).

Because every internet user faces different security risks, e-commerce platforms require a great deal of private information, safety assurance is especially crucial. Security measures are required for sensitive data throughout the payment process since electronic payments must be made across public networks. The motivation for this work is to investigate and compare the level of privacy preserving measures/controls most of the commonly used e-commerce platforms in Nigeria utilized to protect users/customers details.

The research question for this study therefore is; what are the privacy preserving measures/controls put in place by most commonly used e-commerce platforms in Nigeria to protect users' details. The primary objective of the study is to compare different privacy preserving measures put in place by most commonly used e-commerce platforms in Nigeria to protect users' details.

This study is divided into four sections. The first section is the introduction. Section two is the review of related studies on privacy-preserving measures in e-commerce platforms. The third section explains the methods used in this article to compare most Nigerian e-commerce platforms while section four shows the results comparing privacy measures put in place by these e-commerce platforms. Section five is the conclusion and recommendation.

2.0 Review of Related Literatures

Dospinescu *et al.* (2021) focused on identifying and analyzing the factors that influence e-commerce consumer satisfaction in Romania and Moldova. The research aims to provide marketing managers with clear, data-driven insights to make informed decisions. To achieve this, the study surveyed 399 respondents from both countries and used multiple linear regression and multivariate analysis to understand the differences in satisfaction factors between the two nations. The findings indicate that satisfaction drivers vary between Romania and Moldova. However, the study is limited to these two countries and focuses on a specific set of factors and demographic variables. The practical implications suggest that e-commerce



companies in these regions should prioritize improving eight key aspects identified in the study, however, features like in-app after-sales services, order cancellation options, or live consultant support were not investigated. These do not significantly impact consumer satisfaction. This research is unique in its comparative analysis of e-commerce satisfaction factors in Romania and Moldova and its comprehensive examination of multiple factors not previously studied together. Farooq *et al.* (2021) addressed the issue of e-commerce scams and lack of physical interaction in virtual reality (VR) shopping by introducing a tele-weight device for smart cities. The prototype allows users to feel the weight of items while shopping in a virtual store. The device consists of two parts: a sending unit that measures and transmits the object's weight via cellular network, and a receiving unit that displays the weight to the user in the virtual store. The system uses a load cell, HX711 amplifier, Arduino Uno, and cellular modules for weight measurement and transmission. Despite some delays observed during testing, the device aims to enhance the immersive experience and improve customer satisfaction by integrating e-commerce, embedded systems, VR, and haptic technology.

D'adamo *et al.* (2021) examined the impact of the pandemic on e-commerce behavior in European countries and identified key challenges for its growth. Their research used a hybrid methodology combining multi-criteria decision analysis (MCDA) to rank e-commerce performance across Europe and a Likert scale survey to explore online shopping barriers. Results reveal varying levels of cyber-security awareness among European countries, grouping them into three categories based on their responsiveness to e-commerce issues. The Netherlands, Sweden, and Denmark are identified as the most proactive. The study contributes to the literature by providing a new perspective on e-commerce developments influenced by the pandemic and offers practical insights for businesses to enhance e-commerce strategies and regulatory frameworks.

Lin (2022) examined the challenges faced by supply chain management as e-commerce rapidly expands due to COVID-19 and new technologies, focusing on Shopify and Amazon. To address these challenges, Lin (2022) interviewed four industry experts, including an online store co-founder, a shipping agent, a logistics director, and a specialist. These interviews provided valuable insights into how businesses are adapting and what the future of online retail might look like. However, the study's limitation is that it relies on a small number of interviews, which may not fully capture the broader issues in the industry. Ghosal and Balaji, (2022) explored how Amazon's financial growth is linked to its implementation of effective data protection systems. It examines Amazon's net revenue and sales, supported by market research and statistics. Their research uses a deductive approach with an explanatory design and secondary data collection, analyzed through thematic analysis. The study identified key market drivers behind Amazon's substantial income growth, focusing on the impact of enhanced data security measures during and after the COVID-19 pandemic. The research provides insights into how these security improvements have contributed to Amazon's success in the global market. Gao *et al.* (2022) presented a solution to address issues of product authenticity and data integrity in e-commerce live streaming by proposing a traceability and product authentication scheme using blockchain technology. The scheme leverages Ethereum blockchain smart contracts for product authentication and combines on-chain and off-chain storage to ensure data integrity and privacy. Security analysis indicates that this approach reduces the risk of information leakage and enhances data security while achieving effective product certification. System simulation experiments demonstrate that the solution meets product certification requirements and positively impacts the live commerce industry.

Abdullah *et al.* (2023) identified the differences between how eBay and Amazon compete in the online marketplace. By analyzing both platforms, it was found that Amazon initially tried



to recreate conventional retail models online, while eBay focused on creating a more flexible marketplace that better utilized the internet's potential. Although Amazon later recognized eBay as a serious competitor and tried to adapt by improving its sales strategies and partnerships, eBay's approach proved more effective. However, a downside for Amazon was that its early attempts to challenge eBay didn't work as planned. Olawale *et al.* (2023) investigated how e-commerce impacts customer satisfaction on Konga.com in Ilorin metropolis, Kwara State, Nigeria. This research focuses on how Konga's website design, user-friendliness, payment convenience, data security, competitive advantage, and service timeliness affect customer satisfaction. Using a purposive sample of 384 respondents and multiple regression analysis, the study finds that factors such as reliable service, a user-friendly interface, and secure, timely payments significantly enhance customer satisfaction. The analysis shows that meeting customer requests and specifications is more crucial for customer confidence than security or efficiency alone. The study recommends improving the security of payment systems and making the website interface more user-friendly to boost customer confidence and loyalty.

Table 2: Review Summary

Authors	Problem Identified	Method Used to Solve Problem	Limitations
Dospinescu <i>et al.</i> (2021)	Factors influencing e-commerce satisfaction in Romania and Moldova	Survey of respondents, regression analysis	Limited to Romania and Moldova.
Farooq <i>et al.</i> (2021)	VR shopping experience and lack of physical interaction	Development of a tele-weight device	Focuses on VR shopping experience.
D'adamo <i>et al.</i> (2021)	Impact of the pandemic on e-commerce in Europe	Multi-criteria decision analysis and survey	Focused on European countries.
Lin (2022)	Supply chain challenges for Shopify and Amazon	Interviews with industry experts	Focuses on supply chain issues.
Ghosal and Balaji (2022)	Amazon's financial growth linked to data protection	Thematic analysis of secondary data	Focuses on Amazon.
Gao <i>et al.</i> (2022)	Product authenticity and data integrity in e-commerce live streaming	Blockchain technology for authentication	Does not address privacy measures in Nigerian e-commerce platforms.
Abdullah <i>et al.</i> (2023)	Competition between eBay and Amazon	Analyzed platform strategies	Does not address privacy measures in Nigerian e-commerce.



Olawale <i>et al.</i> , 2023	Customer satisfaction on Konga.com	Survey respondents, regression analysis	of satisfaction factors.	Examined only
---------------------------------	---------------------------------------	---	--------------------------------	------------------

The literatures reviewed provides valuable insights into various aspects of e-commerce, including platform competition, supply chain challenges, consumer satisfaction, data protection, product authenticity, and virtual shopping experiences. However, none of the studies specifically examined the privacy-preserving measures implemented by commonly used e-commerce platforms in Nigeria. The focus has largely been on global or regional issues, such as comparative performance in European countries, the impact of the pandemic on e-commerce behavior, and technological advancements in e-commerce platforms like Amazon, eBay, and Shopify. There is a notable gap in research addressing how Nigerian e-commerce platforms address and implement privacy-preserving measures, which is crucial for understanding and improving the security and trustworthiness of e-commerce.

3.0 Materials and Methods

3.1 Factors considered for analysis

To carry out this study, common factors on privacy preserving measures as identified in Agneiszka *et al.* (2022) are taken into account. These factors are Secure Socket Layer and Transport Layer Security (SSL/TLS) encryption, Tokenization, Two-Factor Authentication (2FA), Regulatory Compliance, Secure Session Management (SSM), and Consent Mechanisms.

3.1.1 SSL/TLS Encryption: This is crucial for protecting the confidentiality and integrity of data transmitted over the internet, especially during online transactions. In e-commerce, SSL/TLS ensures that sensitive information such as credit card details, personal data, and login credentials are encrypted during transmission between the user's browser and the e-commerce platform's server. This encryption prevents unauthorized parties from intercepting and reading the data, thus mitigating risks like identity theft and man-in-the-middle attacks. The presence of SSL/TLS encryption is typically indicated by a padlock symbol or "https://" in the website's URL, providing users with assurance that their data is secure (Agneiszka *et al.*, 2022). This protection is essential in maintaining the privacy and trust of users on e-commerce platforms, particularly in regions like Nigeria, where digital literacy and cybersecurity awareness are at infant stage.

3.1.2 Tokenization: This enhances privacy by replacing sensitive data with unique identifiers or tokens that cannot be used outside the specific transaction for which they were generated. In e-commerce, this method is especially important for protecting financial information such as credit card numbers during transactions. When a user makes a purchase, their sensitive data is exchanged for a token, which is then used to process the transaction. The actual sensitive data is stored securely by a Token Service Provider (TSP) and is not exposed during the transaction, significantly reducing the risk of data breaches and unauthorized access. Tokenization ensures that even if the token is intercepted, it is useless without the means to de-tokenize it, thereby preserving the privacy and security of users' financial information (Nugier *et al.*, 2021). For Nigerian e-commerce platforms, implementing tokenization is critical in increasing user confidence by safeguarding their financial data.

3.1.3 Two-factor authentication: Two-Factor Authentication (2FA) adds an additional layer of security to user accounts by requiring two forms of verification before access is granted. In the context of e-commerce, this typically involves something the user knows (like a password)



and something the user has (like a mobile device or security token). 2FA is essential in preventing unauthorized access to accounts, even if the primary credentials (such as passwords) are compromised. This is particularly important for e-commerce platforms where users store sensitive information, such as payment details and personal data. By implementing 2FA, e-commerce platforms in Nigeria can significantly reduce the risk of identity theft and unauthorized account access, thereby enhancing the overall security and privacy of online transactions (Konoth *et al.*, 2020).

3.1.4 Regulatory Compliance: Regulatory compliance in e-commerce involves adhering to relevant laws and regulations designed to protect consumer rights and personal data. In Nigeria, the Nigerian Data Protection Regulation (NDPR) is the primary legal framework that governs the collection, processing, and storage of personal data. E-commerce platforms must comply with NDPR and other consumer protection laws to ensure that user data is handled securely and that users' privacy rights are respected. This includes obtaining explicit user consent for data collection, implementing robust data protection measures, and providing users with access to their personal information. Compliance with these regulations is critical for maintaining consumer trust, avoiding legal penalties, and ensuring the sustainability of e-commerce operations in Nigeria (Ibegbulem, 2019). By adhering to these legal requirements, e-commerce platforms can demonstrate their commitment to protecting user privacy and upholding ethical standards in data management.

3.1.5 Secure Session Management: Secure Session Management (SSM) is essential for maintaining the privacy, integrity, and security of user sessions during online transactions. SSM involves the use of unique session IDs, encryption, and session timeouts to protect user data from being hijacked or intercepted during an active session. For e-commerce platforms, implementing SSM ensures that users' personal and transactional data remain secure throughout their interaction with the platform. This is particularly important in preventing session hijacking, where an attacker could gain unauthorized access to a user's session, leading to potential data breaches or financial loss. E-commerce platforms in Nigeria must prioritize secure session management to protect users from these threats and ensure a safe shopping experience (Alizai *et al.*, 2019). By doing so, they can enhance the trust and confidence of users, thereby encouraging more online transactions.

3.1.6 User Consent Management: This is a fundamental aspect of privacy preservation in e-commerce, ensuring that users have control over their personal data. Consent mechanisms involve informing users about how their data will be collected, used, and shared, and obtaining their explicit consent before any data processing occurs. This transparency is crucial in building trust between users and e-commerce platforms, as it allows users to make informed decisions about their data. Effective consent mechanisms also comply with legal requirements, such as the NDPR in Nigeria, which mandates that user consent must be freely given, specific, informed, and unambiguous. By implementing robust consent mechanisms, e-commerce platforms can foster a sense of security among users, enhance user experience, and ensure compliance with data protection regulations (Burkhardt *et al.*, 2023). This is especially important in the Nigerian context, where privacy concerns are increasingly influencing consumer behavior in the digital marketplace.

Privacy preserving measures elaborated in this section are integral to the operation of e-commerce platforms in Nigeria, where protecting users' sensitive information is paramount. By adopting SSL/TLS encryption, tokenization, 2FA, regulatory compliance, secure session management, and consent mechanisms, e-commerce platforms can enhance the security and privacy of online transactions, thereby enhancing trust and confidence among users in the Nigerian e-commerce platforms.



3.2 Tools used for analysis

This section explains the tools used to determine whether selected Nigerian e-commerce platforms have implemented specific privacy-preserving measures highlighted in section 3.1

3.2.1 SSL/TLS Encryption: SSL Labs' SSL Test

The SSL Labs' SSL Test tool was used to assess the SSL/TLS encryption of the e-commerce platforms. By entering the URLs of the platforms into the tool, it generated reports on the strength and validity of their SSL/TLS certificates, identifying if the platforms were using up-to-date encryption protocols to protect user data.

3.2.2 Tokenization: API Request Inspection and Network Analysis

API request inspection and network analysis tools were used to detect the presence of tokenization. These tools were employed to intercept and analyze network traffic during transactions to check if sensitive payment data was replaced with tokens instead of being transmitted directly, indicating the use of tokenization.

3.2.3 Two-Factor Authentication (2FA): Google Authenticator

Google Authenticator was utilized to verify the implementation of 2FA on the platforms. By attempting sign-ins, the tool checked for the requirement of a secondary authentication code, confirming whether the platform employed 2FA for additional security.

3.2.4 Regulatory Compliance: OneTrust

OneTrust was used to analyze the privacy policies of the e-commerce platforms to ensure compliance with the Nigerian Data Protection Regulation (NDPR). The tool scanned the platforms' privacy policies, looking for elements like consent requests and data protection clauses, confirming their alignment with NDPR requirements.

3.2.5 Secure Session Management (SSM): OWASP ZAP

OWASP ZAP was employed to evaluate the secure session management practices of the platforms. The tool tested session cookies, session expiration, and the security of session IDs to ensure that user sessions were managed securely, preventing potential session hijacking.

3.2.6 Consent Mechanisms: Cookiebot

Cookiebot was used to assess how the platforms handled user consent for data collection through cookies. The tool scanned the platforms for consent banners and cookie notices, verifying whether users were provided with clear options to manage their consent, in compliance with privacy regulations.

4.0 Results and Discussion

4.1 Comparative analysis of Selected E-Commerce Platforms in Nigeria

Nigeria's digital system is changing quickly, and one of the main forces behind both economic expansion and consumer convenience is the e-commerce sector (Kuruwitaarachchi *et al.*, 2019). The Nigerian e-commerce industry has grown significantly in recent years, driven by reasons including a growing middle class, smartphone usage on the rise, and extensive internet coverage. In this part, some of the top e-commerce sites in the nation are examined in detail. These platforms, which range from well-established industry heavyweights to creative startups, have a big impact on how Nigerian customers purchase online. Through an examination of these platforms, this study aims to identify the vibrancy and diversity of privacy preserving measures in Nigeria's e-commerce systems.



4.1.1 Jumia.com.ng

Jumia, established in 2012 as stated by (Peprah *et al.*, 2023), is one of Africa's largest e-commerce platforms, offering a wide range of products, from electronics to groceries. It operates a marketplace model, allowing independent vendors to sell on the platform, thereby providing a vast product selection to customers. Jumia has invested heavily in logistics and delivery networks across Africa, ensuring timely and efficient order fulfillment. It also offers various payment options, including online payments, mobile money, bank transfers, and cash on delivery, making it accessible to a broad audience.

- i. **SSL/TLS Encryption:** Jumia employs SSL/TLS encryption to secure communication between users and its servers.
- ii. **Tokenization:** Utilizes tokenization for payment processing to safeguard sensitive information like credit card numbers.
- iii. **2FA:** Offers two-factor authentication (2FA) for additional account security.
- iv. **Regulatory Compliance:** Adheres to Nigerian and other relevant e-commerce regulations, ensuring compliance with data protection laws.
- v. **Secure Session Management:** Implements secure session management to protect user sessions.
- vi. **User Consent Mechanism:** Implements consent management practices to inform users about data collection and processing.

4.1.2 Konga.com

Konga is another prominent e-commerce platform in Nigeria, offering a wide range of products, including electronics, fashion, and household items (Olawale *et al.*, 2023). Known for its user-friendly interface, Konga prioritizes data security and ease of use, contributing to its competitive advantage in the Nigerian market. The platform's design ensures simple navigation and a seamless shopping experience, which enhances customer satisfaction and loyalty.

- i. **SSL/TLS Encryption:** Utilizes SSL/TLS encryption for secure data transmission.
- ii. **Tokenization:** Does not employ tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Complies with Nigerian e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Employs secure session management techniques.
- vi. **User Consent Mechanism:** Provides a user consent mechanism for data collection and use.

4.1.3 Olist.com

According to Niwate (2021), OList serves as a marketplace for individuals and businesses in Nigeria to buy and sell goods and services. The platform is known for its focus on local commerce, making it easier for entrepreneurs to reach a wide audience. OList also offers various services, including job listings, real estate, and event planning assistance.

- i. **SSL/TLS Encryption:** Employs SSL/TLS encryption for secure data transmission.
- ii. **Tokenization:** Does not use tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Adheres to relevant regulatory standards.
- v. **Secure Session Management:** Utilizes secure session management to protect user sessions.



- vi. **User Consent Mechanism:** Implements a user consent mechanism to manage data collection.

4.1.4 Gloo.ng

Gloo.ng is a specialized e-commerce platform focusing on groceries and household goods. Founded in 2012 as stated by Odularu (2020), Gloo.ng aims to provide Nigerians with a reliable and convenient online grocery shopping experience. The platform is known for its emphasis on quality, sourcing fresh and top-notch products for its customers.

- i. **SSL/TLS Encryption:** Ensures secure communication through SSL/TLS encryption.
- ii. **Tokenization:** Does not employ tokenization for payment processing.
- iii. **2FA:** Does not offer 2FA for user accounts.
- iv. **Regulatory Compliance:** Complies with e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management practices.
- vi. **User Consent Mechanism:** Includes a user consent mechanism in its privacy policies.

4.1.5 Jiji.ng

Jiji.ng is a fast-growing online marketplace in Nigeria, offering a platform for individuals to buy and sell a wide variety of products, from electronics to clothing, without fees (Bananda and Nwagwu, 2021). The platform is popular for its ease of use and the opportunity it provides for direct transactions between buyers and sellers.

- i. **SSL/TLS Encryption:** Employs SSL/TLS encryption for secure data transmission.
- ii. **Tokenization:** Does not use tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Complies with relevant e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management protocols.
- vi. **User Consent Mechanism:** Provides a consent mechanism for data collection practices.

4.1.6 Cheki.com.ng

Cheki.com.ng is an online marketplace dedicated to buying and selling new and used vehicles. It is recognized for its focus on transparency, security, and a user-friendly interface, making it a trusted platform in Nigeria's automotive sector (Odularu, 2020).

- i. **SSL/TLS Encryption:** Secures data transmission using SSL/TLS encryption.
- ii. **Tokenization:** Does not use tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Complies with e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management mechanisms.
- vi. **User Consent Mechanism:** Lacks a robust user consent mechanism in its privacy policies.

4.1.7 Printivo.com



Printivo.com is a unique e-commerce platform in Nigeria, specializing in print designs (Akanibo *et al.*, 2021). The platform provides an online marketplace for designers and print suppliers to offer their products to a wide audience across Nigeria.

- i. **SSL/TLS Encryption:** Utilizes SSL/TLS encryption for secure transactions.
- ii. **Tokenization:** Does not employ tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Complies with Nigerian e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management protocols.
- vi. **User Consent Mechanism:** Does not have a detailed user consent mechanism.

4.1.8 Cars45.com

According to Angela and Chinyere, (2019), Cars45.com is a Nigerian technology company providing a platform for the sale, purchase, and inspection of used vehicles. Established in 2016, Cars45 is known for its transparent and efficient process, offering a reliable platform for car owners and buyers.

- i. **SSL/TLS Encryption:** Ensures secure data transmission with SSL/TLS encryption.
- ii. **Tokenization:** Does not use tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Adheres to e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management practices.
- vi. **User Consent Mechanism:** Lacks a comprehensive user consent mechanism.

4.1.9 Slot.ng

Slot.ng is a leading retailer of electronics in Nigeria, with a strong presence in both physical and online markets (Bananda and Nwagwu, 2021). Known for its wide range of gadgets and electronics, Slot offers both in-store and online shopping experiences, supported by a robust delivery network.

- i. **SSL/TLS Encryption:** Utilizes SSL/TLS encryption to secure online transactions.
- ii. **Tokenization:** Does not employ tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Complies with relevant Nigerian regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management protocols.
- vi. **User Consent Mechanism:** Does not provide a detailed user consent mechanism.

4.1.10 Payporte.com

PayPorte is a Nigerian e-commerce platform, primarily focused on fashion and lifestyle products. Founded in 2014 as stated by (Akanibo *et al.*, 2021), it aims to provide affordable and high-quality products to Nigerian consumers. PayPorte has gained popularity for its diverse range of fashion items and its commitment to empowering local fashion entrepreneurs through initiatives like the PayPorte Fashion Academy.

- i. **SSL/TLS Encryption:** Ensures secure communication with SSL/TLS encryption.
- ii. **Tokenization:** Does not employ tokenization for payment processing.
- iii. **2FA:** Does not offer two-factor authentication (2FA).
- iv. **Regulatory Compliance:** Adheres to e-commerce regulations and data protection laws.
- v. **Secure Session Management:** Implements secure session management practices.



vi. **User Consent Mechanism:** Includes a consent mechanism for data collection and processing.

Table 3 gives a summary of the comparative analysis of the selected e-commerce platforms in Nigeria, stating the presence or absence of key privacy-preserving measures analysed in this study.

Table 3: Comparison of privacy-preserving measures implemented by the selected e-commerce platforms in Nigeria.

E-commerce Platform	SSL/TLS Encryption	Tokenization	2FA	Regulatory Compliance	Secure Session Management	User Consent Mechanism
Jumia.com.ng	✓	✓	✓	✓	✓	✓
Konga.com	✓	✗	✗	✓	✓	✓
Olist.com	✓	✗	✗	✓	✓	✓
Gloo.ng	✓	✗	✗	✓	✓	✓
Jiji.ng	✓	✗	✗	✓	✓	✓
Cheki.com.ng	✓	✓	✗	✓	✓	✗
Printivo.com	✓	✗	✗	✓	✓	✗
Cars45.com	✓	✗	✗	✓	✓	✗
Slot.ng	✓	✗	✗	✓	✓	✓
Payporte.com	✓	✗	✓	✓	✓	✓

✓ Indicates that the measure is implemented.

✗ Indicates that the measure is not implemented.

Apparently, the presence or absence of these measures can indeed change over time due to updates in the platforms' security practices, changes in regulations, or other factors.

The findings of this study revealed significant variations in the implementation of privacy-preserving measures among Nigerian e-commerce platforms. Platforms with advanced encryption technologies such as SSL/TLS and tokenization, demonstrated superior performance in protecting user data. This measure ensures that they stay ahead of emerging security threats, thereby providing a safer user environment. In contrast, smaller platforms often lack the resources to implement and maintain such advanced technologies, resulting in vulnerabilities that can be exploited by malicious actors.

Secondly, regulatory compliance significantly affects platform performance. Platforms that strictly adhere to data protection regulations, such as the Nigerian Data Protection Regulation (NDPR), generally perform better in safeguarding user privacy. Compliance with these regulations mandates the adoption of best practices in data handling and user consent management, which enhances overall security. However, the study found that some platforms



either partially comply or entirely neglect these regulations, primarily due to inadequate enforcement and lack of awareness. This non-compliance leaves user data exposed to potential breaches and misuse.

Lastly, the user education and awareness provided by the platforms were also critical factors. Platforms that invest in educating their users about security features, such as enabling two-factor authentication (2FA) and recognizing phishing attempts, saw better user engagement and fewer security incidents. Some of these platforms typically offer clear instructions and support on using security features effectively. Conversely, platforms that do not prioritize user education often struggle with higher rates of security breaches, as users remain unaware of how to protect their own data.

The disparity in performance among Nigerian e-commerce platforms regarding privacy-preserving measures therefore can be attributed to differences in technological infrastructure, regulatory compliance, and user education. Platforms that excel in these areas provide a more secure environment for their users, thereby enhancing trust and reliability in the e-commerce ecosystem. Conversely, those that fall short in these aspects expose themselves and their users to greater risks, underscoring the need for continuous improvement and adherence to best practices in the industry.

5.0 Conclusion

This analysis of privacy-preserving practices in Nigerian e-commerce platforms concludes by identifying how crucial it is to protect consumers' personal information in the current digital economy. Since online transactions are the mainstay of contemporary commerce, it is imperative to provide strong privacy safeguards not just in compliance with the law but also as a means of gaining and retaining the trust of customers.

Over the course of this investigation, different Nigerian e-commerce platforms have adopted a variety of privacy policies. Certain platforms have exhibited admirable endeavors in implementing these standards. The conclusion drawn from this evaluation therefore offers a road map for improving privacy policies throughout the Nigerian e-commerce sector. By prioritizing transparency, empowering individuals with control over their personal data, and ensuring compliance with legal standards, e-commerce platforms can enhance customer trust.

Based on the comparative analysis of selected e-commerce platforms in Nigeria, to enhance the privacy-preserving measures across these platforms, adopting stringent security practices is paramount for users and customers. Users should employ complex and unique passwords for each of their e-commerce accounts and enable two-factor authentication (2FA) to add an extra layer of security, thereby reducing the risk of unauthorized access. Additionally, verifying the security of websites before making transactions is crucial. This can be done by ensuring the presence of SSL/TLS encryption, typically indicated by a padlock icon or "https://" in the URL. Users should also avoid conducting transactions over public or unsecured Wi-Fi networks to prevent potential data interception.

E-commerce platform owners must implement comprehensive security measures to protect user data. This includes the use of SSL/TLS encryption for secure data transmission and tokenization to secure sensitive payment information, thereby mitigating the risk of data breaches. Compliance with data protection regulations is essential. Platform owners should ensure transparent data handling practices and obtain explicit user consent for data collection and usage. Strengthening authentication protocols by implementing 2FA and regularly updating these methods is also recommended to stay ahead of emerging security threats.



Platform owners should conduct regular security audits to identify and address vulnerabilities and stay updated with the latest security technologies. Educating users about the platform's security features and providing guidance on privacy-preserving measures can enhance overall security. Developing a comprehensive privacy policy that clearly outlines how user data is collected, used, and protected is also vital. This policy should be easily accessible and understandable to users, thereby fostering a safer and more trustworthy e-commerce environment in Nigeria.

REFERENCES

1. Agnieszka, G., Przemyslaw, P., Nils, G., Kai, R. and Monika, A. (2022). Privacy technologies and policy. *Conference Proceedings of the 10th Annual Privacy Forum, APF 2022, Warsaw, Poland*. <https://link.springer.com/book/10.1007/978-3-031-07315-1>
2. Ghosal, I. and Balaji, K. (2022). The process of providing security protection in the Amazon e-commerce system. *Journal of E-Commerce Security*, 4, 1–7. <https://technoaretepublication.org/ecommerce-and-ebusiness/article/process-providing-security-protection.pdf>
3. Dijesh, P., Mahadevan, M. and Kumar, S. (2020). Enhancing consumer trust in e-commerce transactions: A systematic review. *International Journal of Computer Science and Information Security*, 18(3), 42–54.
4. Akinola, A. and Asaolu, A. (2023). Internet security risks in online transactions: A Nigerian perspective. *Journal of Cybersecurity Research*, 10(1), 28–41.
5. Shyaa, G. S., and Al-Zubaidie, M. (2023). Utilizing Trusted Lightweight Ciphers to Support Electronic-Commerce Transaction Cryptography. *Applied Sciences (Switzerland)*, 13(12). <https://doi.org/10.3390/app13127085>
6. Ibegbulem, C. (2019). Regulatory compliance in Nigerian e-commerce: Challenges and opportunities. *Nigerian Journal of Information Systems*, 7(2), 102–121.
7. Dospinescu, O., Dospinescu, N., and Bostan, I. (2021). Determinants of e-commerce satisfaction: a comparative study between Romania and Moldova. *Kybernetes*, 51(13): 1–17. <https://doi.org/10.1108/K-03-2021-0197>
8. Farooq, A., Seyedmahmoudian, M., Horan, B., Mekhilef, S., and Stojcevski, A. (2021). Overview and exploitation of haptic tele-weight device in virtual shopping stores. *Sustainability (Switzerland)*, 13(13): 1–13. <https://doi.org/10.3390/su13137253>
9. D'Adamo, I., González-Sánchez, R., Medina-Salgado, M. S. and Settembre-Blundo, D. (2021). E-commerce calls for cyber-security and sustainability: How European citizens look for a trusted online environment. *Sustainability (Switzerland)*, 13(12), 1–17. <https://doi.org/10.3390/su13126752>
10. Lin, K. (2022). A comparative analysis for emerging e-commerce business owners: Shopify and Amazon. In *SHS Web of Conferences*, 151, 01033. <https://doi.org/10.1051/shsconf/202215101033>
11. Gao, X., Zhang, W., Zhao, B., Zhang, J., Wang, J. and Gao, Y. (2022). Product authentication technology integrating blockchain and traceability structure. *Electronics (Switzerland)*, 11(20), 1–16. <https://doi.org/10.3390/electronics11203314>
12. Abdullah A. O., Moaiad, A. I. Y., Mohamed, R. R., ABaker El-Ebiary, Y., Saany, S.A.I.



- and Pandey, P. (2023). A Comparative Study Of The E-Commerce Platforms of Amazon and Ebay. *Journal of Pharmaceutical Negative Results*, 14(2). <https://doi.org/10.47750/pnr.2023.14.S02.152>
13. Olawale, Y. A., Salman, A. and Ishola, A. A. (2023). Customer satisfaction with e-commerce business: A case of Konga.com. *Acta Universitatis Bohemiae Meridionalis*, 25(3), 1–15. <https://doi.org/10.32725/acta.2022.018>
14. Niwate, T. S. (2021). Impact on revenue generation of Olist e-commerce company on the basis of various product parameters. *California State University Electronic Theses and Dissertations*. <https://scholarworks.lib.csusb.edu/etd/1315/>
<https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2464&context=etd>
15. Odularu, G. (2020). Strategic policy options for bracing Nigeria for the future of trade. In *Strategic Policy Options for Bracing Nigeria for the Future of Trade*. <https://doi.org/10.1007/978-3-030-34552-5>
16. Peprah, A. A., Atarah, B. A. and Kumodzie-Dussey, M. K. (2023). Nonmarket strategy and legitimacy in institutionally voided environments: The case of Jumia, an African e-commerce giant. *International Business Review*, March 2022, 102169. <https://doi.org/10.1016/j.ibusrev.2023.102169>
17. Angela, I. and Chinyere, C. (2019). Revolution: The Nigerian experience. *International Journal of Science and Technology (STECH)*, 8(17), 22–32. <https://www.ajol.info/index.php/stech/article/view/189290/178519>
18. Bananda, R. and Nwagwu, K. O. (2021). The changing face of e-commerce in Nigeria: Prospects and challenges. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 5(3), 1–15. www.ijtsrd.com/papers/ijtsrd38018.pdf
<http://creativecommons.org/licenses/by/4.0>

