impact International Journals and Publications

© IIJP 2026 | Volume 2, Issue 3, pp. 142-155 | ISSN: 2636-4484

# DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS, MALWARE DISTRIBUTION AND ELECTRONIC TRANSACTIONS IN CROSS RIVER STATE, NIGERIA

**Joseph Anthony Odama[1], Dr. Awunghe Achu Ayuk[2], Dr. Barr. Abang Thelma Aya[3], *Dr. Egidi, Stephen Achuen[4] & Eyie Veronica Francis**

*[1,2,3]Department of Criminology and Security Studies, University of Calabar, Calabar, Cross River State, Nigeria.*

*[4]Department of Sociology and Social Work, Arthur Jarvis University, Akpabuyo Cross River State, Nigeria.*

*[5]Department of Sociology, University of Calabar, Calabar, Cross River State, Nigeria*

***Corresponding Author: egidistephen36@gmail.com***

**ARTICLE INFO**

**Article No.:** 0426

**Accepted Date:** 01/06/2026

**Published Date:** 15/07/2026

**Type:** Research

**ABSTRACT**

This study examined the relationship between Distributed Denial-of-Service (DDoS) attacks, malware distribution, and electronic transactions in Cross River State, Nigeria. The study specifically investigated the relationship between Distributed Denial-of-Service (DDoS) attacks and electronic transactions, and established the relationship between malware distribution and electronic transactions. The study was guided by the Technology Acceptance Model (TAM) as a theoretical framework. A descriptive survey research design was adopted. The study was conducted among users of electronic transaction platforms in Cross River State, with an accessible population of 160,000 active users. Using the Taro Yamane (1967) formula, a sample size of 400 respondents was determined and selected through a multi-stage sampling technique. Data were collected using a structured questionnaire. A pilot study produced a Cronbach's Alpha reliability coefficient of 0.82, confirming high internal consistency. Data were analysed using the Pearson Product Moment Correlation at the 0.05 level of significance. The findings revealed a statistically significant relationship between Distributed Denial-of-Service (DDoS) attacks and electronic transactions. The second hypothesis revealed a significant relationship between malware distribution and electronic transactions. The negative correlation coefficients indicate that increasing incidences of DDoS attacks and malware distribution are associated with declining effectiveness, reliability, and user confidence in electronic transaction systems. The study concludes that cyber threats constitute a significant impediment to the sustainability and security of electronic transactions in Cross River State. It therefore recommends the deployment of robust cloud-based and on-premises DDoS mitigation mechanisms, alongside advanced endpoint detection and response (EDR) systems, antivirus solutions, and application whitelisting technologies to strengthen the resilience and security of electronic transaction infrastructures.

**Keywords**: cybercrime, DDoS attacks, malware, electronic transactions and cybersecurity,

## Introduction

Electronic transactions have become an integral component of modern commerce by facilitating online banking, mobile payments, electronic fund transfers, automated teller machine (ATM) services, point-of-sale (POS) payments, and internet-based commercial activities (Adewopo, Azumah, Yakubu, Gyamfi, Ozer & Elsayed, 2024). Unlike conventional crimes, technology-enabled crimes exploit digital platforms, communication networks, information systems, and electronic payment infrastructures to commit offences such as identity theft, phishing, online fraud, ransomware attacks, business email compromise, cyber extortion, financial scams, cryptocurrency fraud, and unauthorized electronic fund transfers. These crimes are increasingly sophisticated because offenders continuously exploit technological innovations to evade detection while targeting individuals, organizations, financial institutions, and governments (Yar & Steinmetz, 2024). Technology-enabled crimes have evolved from isolated hacking incidents into organized and transnational criminal enterprises. Contemporary cybercriminal groups increasingly utilize automation, artificial intelligence, encrypted communication platforms, cryptocurrencies, malware-as-a-service, and dark web marketplaces to facilitate illicit financial activities while concealing their identities. The convergence between technological innovation and organized crime has complicated criminal investigations because perpetrators frequently operate across multiple jurisdictions with sophisticated money-laundering mechanisms that obscure the proceeds of crime (Turner, McCombie, & Uhlmann, 2020).

Another important dimension of technology-enabled crimes is the growing use of cryptocurrencies and blockchain-based financial systems. Although blockchain technology offers transparency and security for legitimate financial activities, criminals have increasingly exploited cryptocurrencies because of their perceived anonymity, decentralized structure, and global accessibility. Criminal networks frequently use digital currencies to facilitate ransomware payments, investment scams, money laundering, online extortion, and cross-border financial crimes. Advances in blockchain forensic investigations have improved the ability of investigators to trace illicit financial flows, although sophisticated laundering techniques continue to present significant enforcement challenges (Khan, 2026). Developing economies face particularly significant challenges because rapid digital financial inclusion is often accompanied by inadequate cybersecurity infrastructure, weak institutional capacity, insufficient public awareness, and evolving legal frameworks. As more citizens adopt electronic banking, mobile payment services, and online commerce, cybercriminals increasingly target inexperienced users through deceptive schemes that exploit trust, limited cybersecurity knowledge, and technological vulnerabilities. Financial institutions consequently experience substantial financial losses, reputational damage, declining customer confidence, and increased operational costs associated with fraud prevention and incident response (Adewopo et al., 2024).

Victims often experience identity theft, emotional distress, privacy violations, disruption of business operations, and loss of confidence in digital financial systems. At the national level, increasing cybercrime undermines investor confidence, threatens financial stability, weakens digital transformation initiatives, and places additional pressure on regulatory agencies and law enforcement institutions responsible for safeguarding electronic commerce. These consequences underscore the necessity for effective cybersecurity governance, comprehensive legal frameworks, technological safeguards, public awareness campaigns, and institutional collaboration among governments, financial institutions, technology providers, and international organizations (Leukfeldt, 2023). Although substantial progress has been made in strengthening cybersecurity policies and electronic payment security, technology-enabled crimes continue to evolve alongside technological innovations. Emerging technologies such as artificial intelligence, machine learning, the Internet of Things

(IoT), deepfakes, and generative AI present both opportunities and new security challenges. Criminals increasingly employ these technologies to automate phishing campaigns, create convincing fraudulent identities, manipulate digital communications, and circumvent conventional fraud detection mechanisms. Consequently, cybersecurity strategies must continuously evolve to address emerging threats while maintaining the efficiency and accessibility of electronic transaction systems (Sorunke, 2026). Assessing technology-enabled crimes within the context of electronic transactions has become increasingly important for understanding the nature, patterns, causes, and implications of cyber-enabled financial offences. Such an assessment provides valuable insights into existing vulnerabilities within electronic transaction systems, evaluates the effectiveness of current preventive measures, and identifies strategies capable of enhancing cybersecurity resilience.

Within Cross River State, electronic transaction services have become increasingly important for public institutions, commercial banks, small and medium-sized enterprises, educational institutions, healthcare facilities, and individual consumers. Despite increasing awareness of cybersecurity challenges in Nigeria, empirical studies focusing specifically on the combined influence of DDoS attacks and malware distribution on electronic transactions within Cross River State remain relatively limited.Therefore, this study seeks to examine the relationship between DDoS attacks, malware distribution, and electronic transactions in Cross River State, Nigeria. The findings are expected to contribute to existing cybersecurity literature while providing practical recommendations for strengthening the security, reliability, and resilience of electronic transaction systems against emerging cyber threats.

**Statement of the Problem**

Electronic transactions provide convenience, speed, and accessibility for individuals and organizations. However, this rapid digital transformation has also exposed users and institutions to sophisticated cyber threats such as Distributed Denial of Service (DDoS) attacks and malware distribution, which threaten the confidentiality, integrity, and availability of electronic transaction systems (Okpa, Ugwuoke, Ajah, Eshiotse, Igbe, Ajor, Ofem, Eteng, & Nnamani, 2022). Distributed Denial of Service (DDoS) attacks disrupt online services by overwhelming computer networks and servers with excessive traffic, making electronic transaction platforms unavailable to legitimate users. Malware including viruses, ransomware, spyware, and Trojans is increasingly used by cybercriminals to steal sensitive financial information, compromise banking applications, manipulate transactions, and cause financial losses to businesses and customers (Tandon, 2020). These cyber threats have become more sophisticated and continue to undermine confidence in digital payment systems across developing economies, including Nigeria ( Ugbaja, 2020).

In Cross River State, the growing reliance on electronic banking, mobile payments, Point-of-Sale (POS) services, and online commercial transactions has created greater exposure to cyberattacks. Previous studies indicate that phishing, malware infections, ransomware, and denial-of-service attacks are among the most common cyber threats experienced by corporate organizations in the state, resulting in operational disruptions, financial losses, and reputational damage (Okpa et al., 2022). Despite increasing awareness of cybersecurity challenges, many organizations and electronic transaction users continue to experience vulnerabilities due to inadequate cybersecurity infrastructure, weak security policies, poor user awareness, and insufficient investment in cyber defense mechanisms (Ugbaja, 2020). While numerous studies have examined cybercrime and electronic banking security in Nigeria generally, there remains limited empirical evidence focusing specifically on the combined effects of DDoS attacks and malware distribution on electronic transactions in Cross River State. This lack of localized evidence creates a knowledge gap for policymakers, financial institutions, businesses, and cybersecurity professionals seeking effective strategies to improve the security and reliability of electronic transaction systems. It

is against this background that this study seeks to investigate the influence of DDoS attacks and malware distribution on electronic transactions in Cross River State, Nigeria.

**Objectives of the study**

a) To investigate the relationship between Distributed Denial of Service (DDoS) and e-transactions
b) To establish the relationship between Malware Distribution and e-transactions

**Research Hypotheses**

1) There is no significant relationship between Distributed Denial of Service (DDoS) and e-transactions
**2)** There is no significant relationship between malware distribution and e-transactions

**Literature review**

**Distributed Denial of Service (DDoS) and e-transactions**

In history of human civilization, financial institutions have significantly increased investments in cybersecurity technologies designed to detect and mitigate DDoS attacks before they disrupt banking operations. These investments include intrusion detection systems, distributed traffic filtering, artificial intelligence-based anomaly detection, cloud-based DDoS mitigation services, threat intelligence platforms, zero-trust architectures, and automated incident response mechanisms. Despite these technological advancements, cybercriminals continuously adapt their attack strategies, creating an ongoing cybersecurity arms race between financial institutions and malicious actors. The banking industry has experienced unprecedented transformation over the last two decades due to continuous advancements in information and communication technologies (ICT). Banking services that were once predominantly delivered through physical branches have increasingly migrated to digital platforms, allowing customers to perform financial transactions regardless of geographical location or time constraints.

Electronic transactions (e-transactions), including internet banking, mobile banking, electronic fund transfers, automated teller machine (ATM) transactions, Point-of-Sale (POS) payments, and online payment gateways, have become indispensable components of modern banking systems. The increasing adoption of these digital financial services has significantly improved operational efficiency, customer convenience, financial inclusion, and economic growth. As financial institutions continue investing heavily in digital infrastructure, uninterrupted availability of these electronic platforms has become essential for maintaining customer satisfaction, institutional competitiveness, and public confidence in the financial system (Khiaonarong & Zheng, 2026). Cybersecurity has therefore become one of the most significant concerns confronting financial institutions globally. As banks increasingly rely on interconnected digital infrastructures, cybercriminals continuously develop advanced attack techniques capable of disrupting financial operations, compromising sensitive information, and undermining customer trust. Among the numerous forms of cyber threats affecting the banking sector, Distributed Denial of Service (DDoS) attacks have emerged as one of the most persistent and damaging attacks because they directly target the availability of banking services rather than merely seeking unauthorized access to confidential information (Odusami, Odusami, Misra, Abayomi-Alli, Abayomi-Alli, & Fernandez-Sanz, 2020). A Distributed Denial of Service attack refers to a cyberattack in which multiple compromised computers, servers, or Internet of Things (IoT) devices simultaneously send enormous volumes of malicious traffic to a targeted server, application, or network infrastructure. The overwhelming volume of requests exhausts available computing resources, rendering legitimate banking services inaccessible to genuine customers. Unlike traditional denial-of-service attacks that originate from a single source, DDoS attacks utilize thousands or even millions of compromised devices distributed across multiple geographical locations, making detection, attribution, and mitigation considerably more challenging. Financial institutions

remain among the primary targets because service availability represents the foundation upon which electronic banking depends (Deressu, Beyene & Gemechu, 2026).

Application-layer DDoS attacks have become particularly difficult to detect because they imitate legitimate customer behavior while consuming significant computational resources within banking applications. This evolution has reduced the effectiveness of traditional firewall-based security mechanisms and necessitated the deployment of artificial intelligence, machine learning, behavioral analytics, and cloud-based mitigation technologies to enhance cyber resilience (Deressu et al., 2026). Electronic transactions represent the operational backbone of modern banking institutions. Every day, millions of customers depend on electronic banking channels to transfer funds, settle bills, receive salaries, purchase goods and services, and conduct commercial activities. The efficiency of these transactions depends on system availability, transaction integrity, confidentiality, authentication, and uninterrupted communication between banking infrastructures. Whenever DDoS attacks disrupt these systems, customers frequently experience delayed transactions, failed transfers, inaccessible mobile applications, interrupted online banking services, ATM downtime, and unsuccessful electronic payments. Such disruptions affect not only customers but also merchants, financial institutions, payment service providers, and national economies that increasingly depend on digital financial ecosystems (Khiaonarong & Zheng, 2026).

Service disruptions may also result in declining customer confidence as consumers increasingly expect uninterrupted access to digital financial services twenty-four hours a day. Repeated cybersecurity incidents may encourage customers to migrate toward competing financial institutions perceived to possess stronger cybersecurity capabilities. Consequently, maintaining continuous service availability has become both an operational necessity and a strategic competitive advantage for banks operating in increasingly digital financial markets (Sokołowski, 2026). As digital banking technologies continue expanding, cybersecurity resilience increasingly determines the reliability and sustainability of electronic financial services (ENISA, 2024). The Nigerian banking industry has equally experienced remarkable digital transformation over the past decade. Driven by the Central Bank of Nigeria's cashless policy, increasing internet penetration, smartphone adoption, financial technology innovations, and growing customer demand for convenient banking services, electronic transactions have become the dominant method of conducting financial activities across the country. Digital payment channels such as mobile banking applications, internet banking platforms, Nigeria Inter-Bank Settlement System (NIBSS) Instant Payments, Unstructured Supplementary Service Data (USSD), POS terminals, and automated teller machines have significantly reduced dependence on physical banking halls while improving financial accessibility for millions of Nigerians (Central Bank of Nigeria, 2024). Statistics from the Nigeria Inter-Bank Settlement System indicate continuous annual growth in electronic payment volumes and transaction values across various payment channels, reflecting increasing public acceptance of digital banking services. This rapid expansion has contributed substantially to financial inclusion, commercial efficiency, and economic development. However, the increased dependence on interconnected digital infrastructures has simultaneously expanded the country's cyber risk exposure. Nigerian financial institutions increasingly experience various forms of cyber threats, including phishing, ransomware, malware, identity theft, insider attacks, business email compromise, and Distributed Denial of Service attacks targeting online banking infrastructures (Nigeria Inter-Bank Settlement System, 2024).

The increasing integration between banks, fintech companies, payment service providers, telecommunications operators, and cloud service providers has created complex digital ecosystems where cybersecurity incidents affecting one institution may produce cascading effects across multiple sectors of the economy (World Economic Forum, 2025).

The emergence of cloud computing, fifth-generation (5G) communication technologies, Internet of Things devices, and open banking frameworks has further complicated cybersecurity management within financial institutions. While these technologies improve banking efficiency and innovation, they simultaneously introduce additional attack surfaces that sophisticated cybercriminals can exploit. Consequently, banks must continuously evaluate emerging threats and implement proactive cybersecurity strategies capable of ensuring uninterrupted electronic transaction services despite increasingly complex attack techniques (World Economic Forum, 2025). Repeated DDoS attacks that interrupt banking services may weaken customer confidence, reduce adoption of electronic banking services, and discourage broader participation in digital financial ecosystems. This challenge becomes particularly significant in developing countries where governments continue promoting cashless economic policies and financial inclusion initiatives. Therefore, strengthening cybersecurity resilience contributes not only to institutional performance but also to national economic development by supporting secure and reliable electronic financial systems.

**Malware Distribution and e-transactions**

Globally, malware attacks have become increasingly organized and financially motivated. The emergence of Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) has transformed cybercrime into a profitable underground economy. These criminal business models allow cybercriminals with limited technical expertise to rent sophisticated malware tools, purchase stolen credentials, and launch attacks against financial institutions and electronic payment systems with minimal effort. Consequently, malware distribution networks have expanded rapidly, increasing both the frequency and sophistication of attacks against businesses, governments, and individuals (Gundur, Topalli, Vakhitova, Liu, Levi, Winter & Baxter, 2026). Nigeria has experienced significant growth in digital payment adoption over the past decade. According to the Central Bank of Nigeria (2024), electronic payment channels including instant transfers, mobile payments, POS transactions, and web-based payment platforms have recorded substantial increases in transaction volumes and values. The rapid expansion of FinTech firms has further accelerated digital financial innovation by providing convenient payment solutions for individuals and businesses. However, this rapid growth has also attracted cybercriminals who exploit vulnerabilities in digital financial systems to perpetrate fraud and malware-related attacks. Reports from cybersecurity organizations indicate that Nigeria remains one of the countries frequently targeted by phishing campaigns, banking Trojans, ransomware, and credential-stealing malware due to its expanding digital economy and increasing internet usage (Nigeria Inter-Bank Settlement System [NIBSS], 2024). One of the most significant threats to e-transactions is banking malware, which is specifically developed to compromise online financial activities. Banking malware infects computers and mobile devices to capture usernames, passwords, one-time passwords (OTPs), debit card information, and other authentication credentials. Some sophisticated banking Trojans are capable of manipulating legitimate banking sessions by modifying transaction details in real time without the user's awareness. Similarly, ransomware attacks can encrypt financial databases, disrupt payment infrastructures, and suspend banking operations until ransom demands are met. These attacks result not only in financial losses but also in operational disruptions, reputational damage, legal liabilities, and declining customer confidence in digital financial services (European Payments Council, 2025).

Malware, a contraction of "malicious software," refers to computer programs intentionally designed to infiltrate, damage, disrupt, or gain unauthorized access to digital systems without the knowledge or consent of users. Malware exists in several forms, including viruses, worms, Trojans, ransomware, spyware, adware, banking malware, keyloggers, rootkits, and fileless malware. Over the past decade, malware has evolved from

relatively simple malicious programs into sophisticated cyber weapons capable of bypassing conventional security mechanisms through encryption, code obfuscation, artificial intelligence-assisted techniques, and zero-day exploits (Demetrio, Coull, Biggio, Lagorio, Armando,& Roli, 2020). Malware distribution refers to the various methods and techniques employed by cybercriminals to spread malicious software across digital devices and networks. Contemporary malware distribution strategies include phishing emails, malicious websites, compromised software updates, infected mobile applications, removable storage devices, exploit kits, social engineering, malicious advertisements (malvertising), and compromised cloud services ( Varlioglu, Elsayed, ElSayed & Oze, 2022).

The rapid digitalization of financial services has made electronic transaction platforms particularly attractive targets because they process highly sensitive financial information and facilitate the movement of monetary assets. Cybercriminals exploit vulnerabilities within these platforms to steal customer credentials, intercept authentication codes, manipulate payment instructions, and gain unauthorized access to bank accounts (Waliullah, George, Hasan, Alam, Munira, & Siddiqui, 2025). The increasing use of smartphones for financial transactions has introduced additional cybersecurity challenges. Mobile banking applications, digital wallets, and contactless payment systems have become attractive targets for mobile malware. Cybercriminals distribute malicious mobile applications disguised as legitimate software to obtain sensitive financial information, intercept SMS verification codes, monitor user activities, and initiate unauthorized financial transactions. As smartphone usage continues to increase in Nigeria, the risk associated with mobile malware has become an important concern for financial institutions, regulators, and consumers (ESET Research, 2025).

Successful malware attacks undermine public trust in electronic payment systems, discourage the adoption of digital financial services, increase cybersecurity expenditure for organizations, and weaken national digital transformation initiatives. Financial institutions are often required to invest heavily in cybersecurity infrastructure, fraud detection systems, employee training, incident response capabilities, and regulatory compliance to mitigate evolving cyber threats. Likewise, governments face increasing pressure to strengthen cybersecurity legislation, enhance inter-agency collaboration, improve cybercrime investigations, and promote cybersecurity awareness among citizens. The issuance of the Cybersecurity Framework for Deposit Money Banks and Payment Service Providers by the Central Bank of Nigeria, the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act, and the establishment of the National Cybersecurity Policy and Strategy. Financial institutions have also adopted multi-factor authentication, biometric verification, artificial intelligence-driven fraud detection systems, endpoint security solutions, and continuous network monitoring to reduce malware-related risks. Nevertheless, the dynamic nature of malware development requires continuous improvement of cybersecurity strategies as attackers constantly develop new methods to evade detection (CBN, 2024). As Nigeria continues to promote a cashless economy and expand digital financial services, understanding the techniques used in malware distribution, their effects on electronic transactions, and the effectiveness of existing security measures is essential for strengthening the resilience of the country's financial ecosystem.

**Theoretical framework**

**Technology Acceptance Model (TAM)**

The Technology Acceptance Model (TAM) was proposed by Fred D. Davis in 1986 The model was developed to explain the factors that influence users' acceptance and adoption of information systems. TAM posits that an individual's intention to use a technological system is primarily determined by two perceptions: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). These perceptions influence users' attitudes toward technology, which

subsequently affect their behavioural intention and actual usage. The Technology Acceptance Model is highly relevant to the study on Distributed Denial-of-Service (DDoS) attacks, malware distribution, and electronic transactions because it explains the mechanism through which cybersecurity threats influence users' willingness to conduct electronic transactions. DDoS attacks disrupt the availability of electronic payment platforms, banking systems, e-commerce websites, and online financial services by overwhelming servers with excessive traffic. When users experience repeated service interruptions, delayed transactions, or system unavailability, they begin to perceive electronic transaction platforms as less useful because the systems fail to perform their intended functions reliably. Similarly, malware distribution including ransomware, spyware, banking Trojans, and keyloggers compromises the confidentiality, integrity, and security of users' financial information. The possibility of financial loss, identity theft, unauthorized access to accounts, or data breaches increases users' perception of risk. These security concerns reduce both the perceived usefulness and the perceived ease of use of electronic transaction systems.

The theory therefore explains why these cybercrimes affect electronic transactions. It suggests that DDoS attacks and malware serve as external variables that negatively influence users' perceptions of system usefulness and ease of use. As these perceptions deteriorate, users' intention to use electronic transaction platforms declines, resulting in lower adoption, reduced transaction volumes, diminished customer trust, and slower growth of digital financial services. Despite its relevance, the Technology Acceptance Model has several limitations. First, the model primarily focuses on individual users' perceptions of usefulness and ease of use while giving limited attention to broader organizational, technological, and environmental factors that influence electronic transactions. Factors such as regulatory policies, institutional trust, cybersecurity governance, and legal protections are not explicitly incorporated into the model. Second, TAM does not directly account for perceived security, privacy concerns, or cyber risk, which are critical determinants of electronic transaction adoption in today's digital environment. Although the model has limitations in addressing broader security and organizational factors, it remains an appropriate framework for understanding how cybersecurity incidents influence the acceptance and continued use of electronic transaction systems.

**Methodology**

This study adopted the descriptive survey research design. The descriptive survey design was considered appropriate because it enables the researcher to obtain relevant information from a representative sample of the population regarding their perceptions, experiences, and opinions on technology-enabled crimes and electronic transactions in Cross River State, Nigeria. The study was conducted in Cross River State, Nigeria. Cross River State is located in the South-South geopolitical zone of Nigeria and consists of eighteen (18) Local Government Areas (LGAs). The state shares international boundaries with the Republic of Cameroon and has experienced significant growth in information and communication technology (ICT), internet usage, mobile banking, electronic commerce, and digital financial services. The target population comprised residents of Cross River State who actively engage in electronic transactions through digital banking platforms, mobile money services, Point-of-Sale (POS) terminals, Automated Teller Machines (ATMs), internet banking, and electronic commerce. For the purpose of this study, the accessible population was estimated at 160,000 adult users of electronic transaction platforms across selected Local Government Areas in Cross River State. The sample size for this study was determined using the Taro Yamane (1967) formula. The sample size is determined as follows:

Where:

n = Sample size

N = Population size

e = Level of precision (sampling error), commonly set at 0.05 (5%) for a 95% confidence level.

Given:

Population (N) = 160,000

Margin of error € = 0.05

Substitute the values into the formula:

$$n = \frac{160,000}{1+160,00\ (0.05)^2}$$

$(0.05)^2=0.0025$

$160,000\times0.0025=400$

$1+400=401$

$$n = \frac{160,000}{401}$$

==399.00

Since sample sizes are expressed as whole numbers, the value is rounded to 400. Therefore, the study adopted a sample size of 400 respondents, which is considered adequate to represent the population of 160,000 at a 5% margin of error and 95% confidence level.

A multi-stage sampling technique was employed in selecting respondents for the study. This technique combined purposive, stratified, proportionate, and simple random sampling methods to ensure that every eligible participant had a fair opportunity of being selected. Stage One: Selection of Senatorial Districts, Cross River State is divided into three Senatorial Districts, namely: Cross River South, Cross River Central and Cross River North. All three Senatorial Districts were included in the study to ensure adequate geographical representation. Stage Two: Selection of Local Government Areas. Using purposive sampling, two Local Government Areas were selected from each Senatorial District based on the high volume of electronic financial transactions, internet penetration, commercial activities, and accessibility. The selected Local Government Areas were: Cross River South (Calabar Municipality and Calabar South). Cross River Central (Ikom and Yakurr). Cross River North (Ogoja and Obudu).

This resulted in a total of six Local Government Areas. Stage Three: Selection of Communities. Within each selected Local Government Area, two communities were selected using simple random sampling, resulting in twelve (12) communities for the study. Stage Four: Selection of Respondents. Eligible respondents included individuals aged 18 years and above who had conducted electronic transactions within the previous twelve months using any recognized digital payment platform. Respondents were selected using systematic random sampling from banks, POS centres, business premises, educational institutions, markets, and public places where electronic transactions are commonly conducted. The sampling interval was determined by dividing the estimated number of eligible respondents at each location by the required sample for that location. Thereafter, every kth eligible respondent was selected until the allocated sample size was achieved. The total sample of 400 respondents was proportionately distributed across the selected Local Government Areas. The instrument used for data collection was a structured questionnaire. The questionnaire items were measured using a five-point Likert scale: Strongly Agree (5), Agree (4), Undecided (3), Disagree (2) and Strongly Disagree (1). The questionnaire was subjected to face and content validity by experts in Criminology, Information Technology, and Research Methodology. Their observations and recommendations regarding clarity, relevance, language, and adequacy of the items were incorporated before the final administration of the instrument. A pilot study was conducted among forty (40) respondents in Akwa Ibom State, which was outside the study area but possessed similar socio-economic characteristics. The data obtained were analyzed using Cronbach's Alpha reliability coefficient. A reliability

coefficient of 0.82 was obtained, indicating that the instrument possessed high internal consistency and was therefore considered reliable for the study. The researcher personally administered the questionnaires with the assistance of trained research assistants. Prior to administration, the purpose of the study was explained to the respondents, and informed consent was obtained. The data obtained was analyzed using Pearson Product Moment Correlation at 0.05 level of significance. Ethical principles guiding social science research were strictly observed throughout the study. Participation was voluntary, and respondents were informed about the objectives of the research before completing the questionnaire.

**Findings**

**Table 1: Distributed Denial of Service and e-transactions**

| Variable | N | Mean | S.D | R-value | Sig. |
|---|---|---|---|---|---|
| Distributed Denial of Service (X) | 400 | 55.84 | 8.72 | | |
| e-transactions (Y) | 400 | 57.16 | 8.95 | -0.648 | 0.000* |

**Significance at 0.05 level, df = 398, critical r-value 0.098**

Since the calculated r-value (-0.648) is greater than the critical r-value (0.098) and the significance value (p = 0.000) is less than 0.05, the null hypothesis is rejected. The calculated correlation coefficient exceeded the critical value of 0.098 at 398 degrees of freedom, indicating that the relationship is statistically significant. Therefore, the study concludes that there is a significant positive relationship between Distributed Denial of Service (DDoS) and e-transactions at the 0.05 level of significance.

**Table 2 Malware Distribution and e-transactions**

| Variable | N | Mean | S.D | R-value | Sig. |
|---|---|---|---|---|---|
| Malware Distribution | 400 | 3.68 | 0.71 | -0.648 | 0.000* |
| e-transactions | 400 | 57.16 | 0.66 | | |

**Significance at 0.05 level, df = 398, critical r-value = 0.098**

The Pearson Product Moment Correlation analysis revealed a moderately strong negative relationship between malware distribution and e-transactions ($r = -0.648$, $p < 0.05$). Since the calculated probability value (0.000) is less than the alpha level of 0.05 and the obtained correlation coefficient exceeds the critical r-value of 0.098 in absolute value, the null hypothesis of no significant relationship is rejected.

**Discussion of findings**

The strong positive correlation suggests that as the level or occurrence of DDoS attacks increases, there is a corresponding increase in their relationship with e-transactions. Zargar, Joshi, and Tipper (2013) reported that DDoS attacks have become one of the most significant cybersecurity threats affecting online business operations due to their ability to overwhelm network resources and interrupt service availability this has corroborated the finding of the study. The result also supports the findings of Buczak and Guven (2016), who noted that growing digitalization and increased electronic transactions provide cybercriminals with more opportunities to exploit network vulnerabilities. Also, Verizon (2024), in its annual Data Breach Investigations Report, emphasized that denial-of-service attacks remain a persistent threat to organizations that rely heavily on online services, particularly within the financial and retail sectors. The implications of these findings are significant for organizations, financial institutions, policymakers, and cybersecurity professionals. Financial institutions should also strengthen incident response plans and invest in resilient network infrastructures capable of maintaining service availability during attacks. As digital financial services continue to expand, strengthening cybersecurity capabilities will be essential to ensuring the availability, reliability, and trustworthiness of e-transaction systems.

This result indicates that an increase in malware distribution is associated with a corresponding decrease in e-transactions. In other words, the widespread presence of

malware discourages individuals and organizations from engaging in electronic transactions due to heightened concerns over financial loss, data theft, and system compromise. The observed negative relationship can be attributed to the disruptive and damaging nature of malware attacks on digital financial systems. The result is consistent with several previous empirical studies. For instance, Kshetri (2021) argued that cyber threats, particularly malware attacks, significantly undermine consumer confidence in electronic commerce and digital payment systems, resulting in lower adoption and transaction rates. Also, Bada and Nurse (2020) reported that malware infections reduce users' trust in online financial platforms because of the increased risk of identity theft, financial fraud, and unauthorized system access. Their study emphasized that security concerns remain one of the strongest barriers to digital financial inclusion. The findings agree with those of Alharbi and Drew (2021), who found that cybersecurity incidents, including malware attacks, negatively influence customers' willingness to use online banking and electronic payment platforms. They concluded that organizations experiencing repeated malware attacks often witness reduced customer engagement and declining transaction volumes because customers seek safer alternatives. Likewise, Roman, Zhou, and Lopez (2018) observed that trust and perceived security are fundamental determinants of electronic transaction adoption, and that cyber threats weaken these perceptions. The finding is also supported by reports from the International Telecommunication Union (2023), which indicate that the increasing sophistication of malware attacks continues to pose serious challenges to the growth of the digital economy. Similarly, the ENISA (2023) reported that malware remains one of the most prevalent cyber threats affecting financial institutions and e-commerce platforms worldwide, contributing to financial losses and reduced consumer confidence in digital payment ecosystems. The implications of this finding are significant for governments, financial institutions, businesses, and consumers.

**Recommendations**

1. Organizations that provide electronic transaction services should implement cloud-based and on-premises DDoS mitigation solutions capable of detecting and filtering malicious traffic in real time. A measurable target is to ensure that DDoS protection systems detect and mitigate at least 95% of attack traffic within five minutes of an attempted attack.
2. Financial institutions and e-commerce platforms should adopt redundant servers, multiple internet service providers (ISPs), and geographically distributed data centers to maintain service availability during attacks. Organizations should aim to achieve a minimum 99.9% service availability even during moderate DDoS incidents.
3. Organizations should perform DDoS stress testing and incident response drills at least twice annually to evaluate the effectiveness of existing defense mechanisms. Performance indicators should include system recovery within 30 minutes after simulated attacks.
4. Organizations should deploy advanced endpoint detection and response (EDR) solutions, antivirus software, and application whitelisting on all systems involved in electronic transactions. A measurable objective is to maintain 100% endpoint protection coverage and ensure security signatures are updated within 24 hours of vendor release.
5. Financial institutions and e-commerce providers should require multi-factor authentication for customers and employees accessing transaction platforms. The target should be 100% MFA implementation for administrative accounts and at least 95% adoption among customer accounts within one year.
6. Employees and customers should receive cybersecurity awareness training focused on phishing, malware, and social engineering attacks at least twice each year.

## Conclusion

This study has demonstrated that Distributed Denial-of-Service (DDoS) attacks, malware distribution, and vulnerabilities in electronic transactions constitute significant cyber threats capable of undermining the security, reliability, and growth of the digital economy. DDoS attacks disrupt the availability of online services by overwhelming systems with illegitimate traffic, resulting in service interruptions, financial losses, and diminished public confidence in digital platforms. Malware distribution further compromises the confidentiality, integrity, and availability of information systems through unauthorized access, data theft, financial fraud, and operational disruption. Similarly, weaknesses in electronic transactions expose individuals, businesses, and institutions to cyber fraud, identity theft, unauthorized financial transfers, and other forms of electronic crime that erode trust in digital payment systems. The findings underscore the interconnected nature of these cyber threats, as each exploits weaknesses in technological infrastructure, human behavior, and organizational security practices. In the context of Cross River State, the practical implications of these findings are substantial. As government agencies, financial institutions, educational institutions, healthcare facilities, and private businesses increasingly rely on digital platforms to deliver services and conduct electronic transactions, the consequences of cyberattacks become more severe. Successful DDoS attacks could disrupt essential government services, banking operations, educational portals, and healthcare information systems, thereby affecting service delivery and economic activities. Therefore, for Cross River State to maximize the benefits of digitalization and electronic commerce, greater investment in cybersecurity infrastructure, skilled cybersecurity personnel, public awareness campaigns, and stronger collaboration among government agencies, financial institutions, telecommunications providers, educational institutions, and law enforcement agencies is essential. Ultimately, mitigating the risks associated with DDoS attacks, malware distribution, and insecure electronic transactions is not merely a technical necessity but a strategic imperative for safeguarding digital assets, ensuring business continuity, promoting financial inclusion, and sustaining economic growth in Cross River State.

**References**


Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). *A comprehensive analytical review on cybercrime in West Africa*. arXiv. https://arxiv.org/abs/2402.01649

Akinyemi, I. O., Ogundele, O. S., & Ojo, A. O. (2022). Cybersecurity challenges and electronic banking fraud in Nigeria. *International Journal of Information Security, Privacy and Digital Forensics, 6*(2), 45–60.

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks. In *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00005-3

Bekkers, L., Snaphaan, T., & Leukfeldt, R. (2026). Examining financial trails of online frauds and money laundering choices of cybercriminals. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-026-09663-2

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Central Bank of Nigeria. (2024). *Annual report and statement of accounts 2024*. https://www.cbn.gov.ng/documents/annualreports.asp

Demetrio, L., Coull, S. E., Biggio, B., Lagorio, G., Armando, A., & Roli, F. (2020). *Adversarial EXEmples: A survey and experimental evaluation of practical attacks on machine learning for Windows malware detection*. arXiv. https://arxiv.org/abs/2008.07125

Deressu, T. F., Beyene, A. M., & Gemechu, A. Y. (2026). A survey of application layer distributed denial of service detection: Approaches, models, and datasets. *Artificial Intelligence Review, 59*, Article 139. https://doi.org/10.1007/s10462-026-11234-0

Douligeris, C., & Serpanos, D. N. (2007). *Network Security: Current Status and Future Directions*. Wiley-IEEE Press. https://doi.org/10.1002/9780470167229

European Payments Council. (2025). *Payments threats and fraud trends report 2025*. https://www.europeanpaymentscouncil.eu

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.itu.int/itu-d/sites/pub-gci/

Gundur, R. V., Topalli, V., Vakhitova, Z., Liu, H. K., Levi, M., Winter, C., & Baxter, A. L. A. (2026). The commercialization of ransomware: From spray-and-prey to big game hunting to the ransom bazaar. *Crime & Delinquency*. https://doi.org/10.1177/00111287261440146

IBM. (2024). *Cost of a Data Breach Report 2024*. https://doi.org/10.1109/SURV.2013.031413.00127

International Telecommunication Union. (2023). *Global Cybersecurity Index 2023*. https://www.itu.int/itu-d/sites/pub-gci/

Khan, M. (2026). Uncovering cryptocurrency-enabled sextortion: A blockchain forensic analysis of transactions and offender laundering tactics. *Information, 17*(3), 236. https://www.imf.org/en/Publications/WP

Khiaonarong, T., & Zheng, S. (2026). *The rise of cyber events and digital fraud in the financial sector* (IMF Working Paper No. 2026/062).

Kshetri, N. (2021). *Cybercrime and Cybersecurity in the Global South*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-74743-6

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). *Cybercriminal networks: Origins, growth and criminal capabilities*. Springer. https://doi.org/10.1007/978-94-6265-177-0

Leukfeldt, R. (2023). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review, 49*, 105858. https://doi.org/10.1007/978-94-6265-177-0

Nigeria Inter-Bank Settlement System. (2024). *Annual payment system statistics report*. https://nibss-plc.com.ng

Odusami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., & Fernandez-Sanz, L. (2020). A survey and meta-analysis of application-layer distributed denial-of-service attack. *International Journal of Communication Systems, 33*(17), e4603. https://doi.org/10.1002/dac.4603

Okpa, J. T., Ugwuoke, C. U., Ajah, B. O., Eshiotse, E., Igbe, J. E., Ajor, O. J., Ofem, N. O., Eteng, M. J., & Nnamani, R. G. (2022). Cyberspace, black-hat hacking and economic sustainability of corporate organizations in Cross River State, Nigeria. *SAGE Open, 12*(3). https://doi.org/10.1177/21582440221121588

Sokołowski, M. (2026). Evaluating cyber attacks on central banks: Identification of trends in cyber threat landscape. *Computers & Security, 160*, 104742. https://doi.org/10.1002/dac.4603

Sorunke, O. (2026). Emerging trends in cybercrime and digital fraud: A critical appraisal. *International Journal of Latest Technology in Engineering, Management & Applied Science, 15*(1).

Tandon, R. (2020). *A survey of distributed denial of service attacks and defenses*. arXiv. https://arxiv.org/abs/2008.01345

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Analysis techniques for illicit Bitcoin transactions. *Frontiers in Computer Science, 2*, Article 600596.

Ugbaja, M. M. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice, 62*, 100415.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Varlioglu, S., Elsayed, N., ElSayed, Z., & Ozer, M. (2022). *The dangerous combo: Fileless malware and cryptojacking*. arXiv. https://arxiv.org/abs/2203.03175

Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). *Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review*. arXiv. https://arxiv.org/abs/2501.09032

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press. https://doi.org/10.1002/9780745634203

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Yar, M., & Steinmetz, K. F. (2024). Reconsidering crime and technology: What is this thing we call cybercrime? *Annual Review of Law and Social Science, 20*, 369–385. https://doi.org/10.1146/annurev-lawsocsci-120223-102438

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against Distributed Denial of Service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127